Hajautetuista palvelunestohyökkäyksistä ja esineiden internetistä

Juha J. Kari

Tampereen yliopisto
Luonnontieteiden tiedekunta
Tietojenkäsittelyoppi
Pro gradu -tutkielma
Ohjaaja: Erkki Mäkinen
Heinäkuu 2017

Tampereen yliopisto
Luonnontieteiden tiedekunta
Tietojenkäsittelyoppi
Juha J. Kari: Hajautetuista palvelunestohyökkäyksistä ja esineiden internetistä
Pro gradu -tutkielma, 39 sivua
Heinäkuu 2017

Hajautettu palvelunestohyökkäys (distributed denial of service attack, DDoS) tarkoittaa tilannetta, jossa hyökkääjä pyrkii lamauttamaan tietoverkossa tarjolla olevan palvelun käyttäen apunaan useita hyökkäysagentteja – tällaiset hyökkäykset ovat saaneet julkisuutta viime vuosina.

Esineiden internetillä (Internet of Things, IoT) tarkoitetaan verkotettuja älykkäitä laitteita, jotka ovat yhteydessä internetiin. Verkotetut laitteet muuttuvat yhä pienemmiksi ja ne ovat yhä useammin jatkuvasti yhteydessä internetiin.

Tässä tutkielmassa tutkitaan kirjallisuuden perusteella palvelunestohyökkäysten tekniikkaa ja torjuntatapoja. Esineiden internetin laitteita tarkastellaan sekä hyökkäysten kohteina että hyökkäyslaitteina.

Avainsanat ja -sanonnat: DDoS, palvelunestohyökkäykset, IoT, esineiden internet.

Sisällys

1. Johdanto

Elämme yhteiskunnassa, jossa suuri osa erilaisista ihmisten käyttämistä palveluista on jo digitalisoitu ja siirretty verkkoon. Yhä uusia palveluja siirretään verkkoon – tai ainakin verkkoon siirtämisestä keskustellaan. Ensimmäisten joukossa fyysisestä maailmasta verkkoon siirtyivät 1990-luvulla kuluttajien pankkipalvelut. Verkossa toimivat myös esimerkiksi kirjastopalvelut, sähköiset reseptit, tiedotusvälineet ja erilaiset viestintäsovellukset. Viihdepalveluista mainittakoon elokuvien ja musiikin suoratoistopalvelut, jotka ovat vähitellen korvaamassa fyysisiä tallenteita, kuten CD-, DVD- ja Blu-ray-levyjä.

Eräs syy palveluiden digitalisoimiseen on pyrkimys vähentää paperisia asiakirjoja. Myös Suomessa valtio aikoo pian luopua paperikirjeistä. Kela, Verohallinto, Trafi ja muut virastot lopettavat paperikirjeiden lähettämisen kansalaisille vuonna 2018, jos hallituksen aikataulu pitää. Muutoksen myötä kansalaisten on avattava itselleen digipostilaatikko viranomaisten kanssa asioimiseen. [Kallio, 2016]

Joissakin maissa, kuten Virossa, myös vaalien äänestysjärjestelmiä on muutettu verkkopohjaisiksi. Suomessa on tähän mennessä korostettu perinteisen lippuäänestyksen turvallisuutta verrattuna sähköiseen äänestämiseen. Suomessa järjestettiin syksyn 2008 kunnallisvaaleissa kolmen kunnan alueella sähköinen äänestyskokeilu, jossa tosin ei hyödynnetty internetiä siten, että kotoa äänestäminen olisi ollut mahdollista. Äänestyskokeilussa ääni annettiin tähän tarkoitukseen suunnitellulla laitteella virallisella äänestyspaikalla. [Karhumäki et al., 2008]

Digitaalisessa yhteiskunnassa verkottumisella tavoitellaan tehokkuuden lisäämistä ja laitteiden uusia käyttömahdollisuuksia. Esimerkiksi aiemmin matkapuhelin oli vain laite puhumiseen sekä tekstiviestien lähettämiseen ja vastaanottamiseen. Nykyään älypuhelimella voidaan käyttää monenlaisia WWW-selaimen kautta käytettävissä olevia palveluita sekä varta vasten hyötykäyttöä ja viihdettä varten suunniteltuja sovelluksia. Samoin televisio oli aiemmin vain vastaanotin, mutta älytelevisioiden aikakaudella laitteessa on myös verkkoyhteys. Joissakin älytelevisioissa on kamera internetin videopuheluita varten, kun taas toisissa on tuki elokuvien suoratoistopalveluille. Nämä uudet palvelut eivät toimisi televisiossa ilman internet-yhteyttä.

Ihmisillä on tapana muodostaa luottamussuhde palveluihin, jotka ovat pitkäaikaisen kokemuksen perusteella olleet toimivia, helppokäyttöisiä ja luotettavia. Joissakin tapauksissa yritysten asiakkailleen tarjoamille verkkopalveluille ei ole enää tarjolla fyysisessä maailmassa toimivia vaihtoehtoja, jotka olisivat tarpeen vaatiessa myös varajärjestelmiä digitaalisen palvelun ollessa syystä tai toisesta poissa käytöstä. Esimerkiksi eräs kotimainen pankki ei tarjoa mahdollisuutta maksaa laskuja pankin toimipaikoissa, vaan ainoa tapa maksamiseen on verkkopankki, joka toimii sekä WWW-selaimen että älypuhelinsovelluksen avulla.

Digitaalisten palveluiden ajateltu tarkoitus on helpottaa tyypillisten palveluiden käyttöä, lisätä itsepalvelua ja lisätä tehokkuutta verrattuna fyysisen maailman perinteisiin palveluihin. Näiden

palveluiden saatavuutta vastaan suunnatut hajautetut palvelunestohyökkäykset ovat yleistyneet 2000-luvulla, ja niiden aiheuttamat vahingot ovat lisääntyneet.

1.1. Esineiden internetistä

Esineiden internetillä (Internet of Things, IoT) tarkoitetaan verkotettuja älykkäitä laitteita, jotka ovat yhteydessä internetiin. Verkotetut laitteet muuttuvat yhä pienemmiksi ja ne ovat yhä useammin jatkuvasti yhteydessä internetiin. Laitteesta riippuen niitä voidaan etäohjata verkon välityksellä tai ne ottavat itse yhteyksiä internetissä oleviin palvelimiin ja pilvipalveluihin. Esineiden internetin mahdollisuudet ovat suuret, koska sen laajamittainen käyttöönotto mahdollistaa suuren laitemäärän verkottumisen sekä etäohjattavuuden. Esineiden internet tuo myös suuria uhkia, mikäli laitteet ovat haavoittuvia tietoturva-aukkojen vuoksi tai jos niiden toimintaa voidaan häiritä palvelunestohyökkäyksillä.

Esineiden internetissä älykkäät laitteet voivat viestiä keskenään ja toimia näkymättömästi käyttäjän puolesta. Tietoturvaongelmia on odotettavissa lisää laitteiden määrän kasvaessa. Murretut esineiden internetin laitteet voidaan valjastaa hajautettuun palvelunestohyökkäykseen hyökkäysagenteiksi. Tekniikka ja Talous -lehden uutisen mukaan tietoturvatutkija Brian Krebsin KrebsOnSecurity-sivustoa vastaan hyökättiin 145000 kameralaitteen suorittamalla hajautetulla hyökkäyksellä, joka tuotti haittaliikennettä jopa 620 gigatavua sekunnissa. Myöhemmin raportoitiin tätäkin suuremmasta hyökkäyksestä, joka tuotti haittaliikennettä 1,1 teratavua sekunnissa. [Tekniikka ja talous, 2016]

Krebs [2016a] raportoi Twitterissä lokakuussa 2016, että aiemmin kuvaamiini ennätysmäisiin palvelunestohyökkäyksiin tarkoitetun Mirai-nimisen IoT-bottiverkon lähdekoodi on julkaistu. Mirai oli lokakuussa 2016 toinen kahdesta haittaohjelmaperheestä, joita käytettiin IoT-pohjaisten hajautettujen palvelunestohyökkäysten toteuttamiseen. Toinen yleinen IoT-haittaohjelma oli tuolloin Bashlight [Krebs, 2016b].

F-Secure-tietoturvayhtiön tutkimusjohtaja Mikko Hyppönen kertoi Iltasanomien uutisessa [Iltasanomat, 2016], että nyt on astuttu uuteen aikakauteen: ”IoT:llä [esineiden internetillä] on nyt saatu aikaan oikeita ongelmia. Enää ei ole kyse tulevaisuudella pelottelusta.” Hyppönen viittasi siihen, että Mirai oli ensimmäisten joukossa oleva esineiden internetin laitteita hyödyntävä palvelunestohyökkäyksiä tekevä haittaohjelma, jonka lähdekoodi on julkaistu internetissä.

Tekniikka ja talous -lehden verkkosivulla raportoitiin helmikuussa 2017, että Mirai-haittaohjelma riehui yhä Suomessakin ja satoja laajakaistaliittymiä oli jouduttu sulkemaan. Uutisen mukaan Mirain leviäminen onnistui, koska kotilaitteissa oli usein käytössä tehtaalla määritellyt oletusarvoiset etähallintaliittymän tunnukset (kuten ”admin”) ja salasanat (kuten ”default”). [Tekniikka ja talous, 2017]

Tietoviikko-lehti uutisoi artikkelissaan TV-tikusta, joka saattaa vaarantaa koko kodin tietotekniset laitteet, koska siinä on tietoturva-aukko, jonka kautta ulkopuolinen hyökkääjä voi saada

hallintaansa langattoman lähiverkon kaiken liikenteen ja kaikki siihen yhteydessä olevat laitteet. Tämä mahdollistaa lähiverkon kaappaamisen palvelunestohyökkäyksiin. [Tietoviikko, 2016a]

1.2. Palvelunestohyökkäyksistä

Palvelunestohyökkäyksen (denial of service attack, DoS) tarkoituksena on saattaa tietojenkäsittelyresurssi saavuttamattomaksi sen luvallisille käyttäjille. Hajautettu palvelunestohyökkäys (distributed denial of service attack, DDoS) tarkoittaa tilannetta, jossa hyökkääjä pyrkii lamauttamaan tietoverkossa tarjolla olevan palvelun käyttäen apunaan useita – tyypillisesti tuhansia – hyökkäysagentteja. [Loukas and Öke, 2010]

Palveluneston tapoja ovat esimerkiksi seuraavat [Viestintävirasto, 2007; Web-opas, 2012]:

1. Tietojenkäsittelyresurssien – kuten kaistanleveyden, levytilan tai prosessoriajan – kuluttaminen.
2. Konfiguraatioinformaation – kuten reititysinformaation – häirintä.
3. Tilainformaation häirintä. Esimerkiksi toivomaton TCP-istuntojen resetointi.
4. Fyysisten verkkokomponenttien häirintä.
5. Luvallisten käyttäjien ja verkkokohteen välisen kommunikaatiomedian tukkiminen.

DDoS-hyökkäys kohdistuu tyypillisesti seuraaviin kohteisiin: WWW-palvelimet, nimipalvelimet (DNS), juuripalvelimet (root DNS), tietyn käyttöjärjestelmän TCP-pino ja tietyn käyttöjärjestelmän ICMP (Internet Control Message Protocol) -toteutus.

Viestintäviraston CERT-FI-palvelun Tietoturva Nyt! -artikkeli toukokuulta 2007 jakaa palvelunestohyökkäykset toteuttamisvälineensä mukaan kolmeen luokkaan [Viestintävirasto, 2007]:

1. Botnetillä, eli etähallittavalla haittaohjelmalla, haltuun otettujen tietokoneiden verkostolla suoritettu hyökkäys.
2. Itsestään verkossa leviävällä madolla toteutettu hyökkäys.
3. Tiedostonjakoon normaalisti käytettävien vertaisverkkojen avulla toteutettu hyökkäys.

Sekä hajautetuilla että perusmuotoisilla palvelunestohyökkäyksillä voi olla tuhoisia seurauksia internetin ja sen palvelujen toiminnalle. Kaupallisten verkkopalvelujen tarkoituksena on tuottaa voittoa omistajilleen, mutta niiden toiminnan lamaantuessa luvallisten käyttäjien pääsy palveluihin estyy ja kaupankäynnin tavoitteena olevat voitot jäävät saamatta tai asiakkaat ovat tyytymättömiä toimimattomiin palveluihin.

Palvelunestohyökkäyksillä voidaan tavoitella pienempiä tai suurempia vahinkoja. Pienistä vahingoista esimerkkinä on verkkopelien palvelimien ylikuormittaminen siten, että pelaajat eivät pääse suosikkipelinsä pariin. Skaalan toinen ääripää on valtioiden kriittisten verkkopalveluiden – kuten vaalien äänestysjärjestelmien – häiritseminen.

Palvelunestohyökkäysten ainoa haitta ei ole palvelun saattaminen käyttökelvottomaksi, vaan niistä voi olla erilaisia taloudellisia haittoja niin palvelun omistajalle kuin asiakkaillekin. Kuitenkin eräs suurimmista hyökkäysten haitoista on hyökkäyksen kohteeksi joutuneen organisaation asiakkaiden luottamuksen mureneminen, kun tavoiteltu palvelu ei olekaan enää käytettävissä.

Hyökkäykset voivat olla pelkkää kiusantekoa niiden kohdetta vastaan, mutta hyökkäyksillä voidaan tavoitella myös uhrin kiristämistä lupaamalla tälle hyökkäysten loppuvan, kun uhri suostuu maksamaan tietyn summan rahaa hyökkääjälle – usein bitcoineina. Toisaalta hyökkäyksillä voi olla myös sotilaallisia tarkoituksia, kun hyökkääjä on valtiollinen taho, joka haluaa haitata toisen valtion kriittisen infrastruktuurin toimintaa.

Palvelunestohyökkäykset ovat rutiiniaseita kyberrikollisten välineistöissä. Niitä käytetään usein yritysten kiristämiseen – palvelunestohyökkäys luvataan lopettaa, kun yritys maksaa lunnaat. Tällaisen hyökkäyksen tekijää tai tekijöitä on usein vaikea jäljittää.

Helsingin Sanomat otti lokakuussa 2016 pääkirjoituksessaan kantaa sähköisten äänestysten alttiuteen ulkopuolisille hyökkäyksille. Lehden mukaan paperilapuilla käytävät vaalit ovat tehottomat ja vanhanaikaiset, mutta ne ovat kuitenkin turvassa poliittiselta kyberrikollisuudelta, kuten palvelunestohyökkäyksiltä. Lehti muistuttaa vuoden 2008 kuntavaalien sähköisestä äänestyskokeilusta, joka epäonnistui ongelmien vuoksi, ja vaalit jouduttiin uusimaan. [HS, 2016]

Aiemmin hajautettuihin palvelunestohyökkäyksiin käytettiin kaapattuja PC-tietokoneita, mutta uusin trendi on esineiden internetin laitteiden murtaminen ja valjastaminen hajautettuihin hyökkäyksiin [Jing et al., 2014]. Esineiden internetin laitteiden määrä on jatkuvassa kasvussa ja laitteiden tietoturva on tähän asti ollut vaihtelevan tasoista, monesti jopa kehnoa. Yritykset tuovat markkinoille jatkuvasti uusia verkkoon liitettäviä tuotteita, mutta niiden tietoturvaan ei ole aina kiinnitetty tarpeellista huomiota.

Lain kannalta palvelunestohyökkäyksessä on kyse tietojärjestelmän häirinnästä. Erityisen tuntuvaa haittaa aiheuttava hyökkäys on törkeää tietojärjestelmän häirintää. Rikoslain 5 a §:n mukaan:

> Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Rikoslain 5 b §:n mukaan:

> Jos tietojärjestelmän häirinnässä
>
> 1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai
>
> 2) rikos tehdään erityisen suunnitelmallisesti
>
> ja tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietojärjestelmän häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

Palvelunestohyökkäysten yleistyttyä erityisesti 2000-luvun alkuvuosina hyökkäyksiä raportoitiin tiedotusvälineissä runsaasti sekä kotimaasta että ulkomailta. Näinä vuosina hyökkäyksiä suorit-

taneet henkilöt onnistuivat usein pysyttelemään piilossa, joten oikeustapauksia erityisesti Suomesta löytyy varsin vähän. Uudelleen palvelunestohyökkäykset nousivat esille mediassa vuosina 2014-2016, kun esineiden internetin laitteita alettiin käyttää hyökkäyksissä

Pulliaisen [2016] mukaan: datamäärän avulla tehtävien tietoturvahyökkäysten voimakkuus on kasvanut merkittävästi kuluvan vuoden 2016 aikana. Viestintäviraston mukaan volyymihyökkäyksissä on tapahtunut vuoden 2016 aikana kymmenkertainen hyppäys.

Ciscon arvion mukaan internetissä oli vuonna 2016 kiinni arviolta 17 miljardia eri laitetta ja vuonna 2020 määrä ylittää jo 25 miljardia. Näistä laitteista vuoden 2016 syksyn suureen palvelunestohyökkäykseen saatiin valjastettua noin 100000 saastunutta laitetta, joten kyseessä oli varsin pieni osa kaikista verkon laitteista. [Pulliainen, 2016]

Viestintäviraston kyberturvallisuuskeskuksen johtava asiantuntija Kauto Huopio arvioi, että vuoden 2016 syksyn hyökkäys ei jää viimeiseksi tämän tyyppiseksi tapaukseksi. F-Securen tutkimusjohtaja Mikko Hyppönen pitää vieläkin laajempaa hyökkäystä teknisesti mahdollisena, mutta motiivia tuollaiseen on vaikea löytää. [Pulliainen, 2016]

Erilaisia motiiveja palvelunestohyökkäysten toteuttamiseen ovat muun muassa [Pulliainen, 2016]:

1. Teinien näyttämisen- ja kokeilunhalu. Puhutaan ns. skriptilapsista (script kiddies), jotka saavat käyttöönsä valmiita hyökkäystyökaluja ja toteuttavat niillä pienellä vaivalla suuriakin hyökkäyksiä.
2. Verkkorikollisten rahan ansaitsemisyritykset. Ammattirikolliset pyrkivät esimerkiksi kiristämään yrityksiä uhkaamalla estävänsä näiden verkkopalveluiden toiminnan. Rikolliset vaativat tyypillisesti yrityksiltä rahaa bitcoin-valuuttana, jotta palvelunestohyökkäys jätettäisiin toteuttamatta.
3. Terroristijärjestöjen – kuten Isiksen – yritykset rauhan tasapainon horjuttamiseen. Toistaiseksi esimerkkinä mainitun Isiksen tekninen osaaminen on ollut läntisiä toimijoita heikompaa.
4. Valtiollisesti johdettujen toimijoiden hyökkäykset, joilla voidaan testata hyökkäyksen kohteen puolustuskykyä ja kartoittaa heikkouksia.

Viestintäviraston mukaan, tyypillinen palvelunestohyökkäys on kooltaan muutamia gigabittejä sekunnissa ja Suomessa sellaisia nähtiin vuoden 2016 aikana tuhansia. Lähes neljä viidesosaa Suomessa koetuista palvelunestohyökkäyksistä oli kestoltaan alle 15 minuuttia. Tässä on kuitenkin otettava huomioon, että hyökkäyksiä voidaan tehdä useita peräkkäin. Vain noin 2 prosenttia Suomessa koetuista palvelunestohyökkäyksistä kesti yli tunnin. [Pulliainen, 2017; Viestintävirasto, 2017]

1.3. Katsaus työn sisältöön

Tässä tutkielmassa käsitellään palvelunestohyökkäyksiä yleisesti ja erityisesti esineiden internetin laitteisiin liittyvänä ilmiönä. Työn tarkoitus on olla katsaus aiheeseen liittyvään kirjallisuuteen ja samalla helppolukuinen johdanto esineiden internetin laitteiden turvallisuuteen liittyviin seikkoihin. Kirjallisuudesta käsitellään erityisesti erilaisia hyökkäystyyppejä ja niiden luokitteluja.

Tutkielmassa esitellään jotakin suojautumismenetelmiä palvelunestohyökkäyksiltä. Palvelunestohyökkäyksiltä voidaan suojautua esimerkiksi sisällönvälitysverkolla (engl. content delivery network, CDN). Kohdepäässä palveluneston vaikutuksia voidaan lieventää kuormantasauksella ja klusteroinnilla. Toinen lähestymistapa suojautumiseen on haittaliikenteen suodattaminen pois lähtöpäässä.

Luku 2 käsittelee palvelunestohyökkäysten perusasioita, kuten niiden tarkoitusta ja hyökkäyksen vaiheita.

Luvussa 3 käsitellään palveluneston teoriaa, kuten internetin ja esineiden internetin tekniikkaa, palveluneston piirteitä, haavoittuvuuksia ja hyökkäystyyppien luokittelua.

Luvussa 4 esitellään kirjallisuuden pohjalta tapoja palvelunestohyökkäyksiltä suojautumiseen.

Luku 5 käsittelee palveluneston historiaa ja toteutuneita hyökkäyksiä menneinä vuosina.

Luvussa 6 esitellään palvelunestohyökkäysten tuoreinta tilannetta Suomessa viimeisimpien julkisuudessa esillä olleiden tapausten valossa.

Luvussa 7 käsitellään työkaluja palvelunestohyökkäyksien tutkimiseen ja kohteita hyökkäyksille sekä esineiden internetiä hyökkäysten kohteena ja lähteenä. Painopiste on yleisesti tunnetuissa sovelluksissa ja verkkopalveluissa.

Luku 8 sisältää lyhyen yhteenvedon tutkielmassa käsitellyistä aiheista.

2. Palvelunestohyökkäyksistä

2.1. Palvelunestohyökkäyksien tarkoitus

Palvelunestohyökkäysten tavoitteena on häiritä laillista toimintaa, kuten esimerkiksi WWW-sivujen selaamista, verkkoradion kuuntelua tai verkkopankin käyttämistä [Mirkovic et al., 2004]. Palveluneston vaikutus saavutetaan lähettämällä kohteeseen viestejä, jotka häiritsevät sen toimintaa. Hyökkäyksessä on lähdepää, josta hyökkäys tehdään, ja kohdepää, johon hyökkäys kohdistuu. Hyökkäysliikenteen määrästä riippuen häiriöstä voi kärsiä kohteena oleva yksittäinen palvelu, koko palveluntuotantoverkko, teleyrityksen asiakasliittymä tai jopa teleyrityksen runkoverkko [Viestintävirasto, 2016c].

Palvelunestohyökkäysten aiheuttamat vahingot voivat olla taloudellisia. Lisäksi ongelmat ovat usein käytännöllisiä – palvelunestohyökkäyksen kohde voi muuttua hyökkäyksen aikana käyttökelvottomaksi, jolloin sen luvalliset käyttäjät ovat vailla tarvitsemaansa palvelua.

Hajautettujen palvelunestohyökkäysten on ajateltu olevan vain *tietoturvaongelma*, mutta se on ensisijaisesti *skaalautuvuusongelma* [Chung, 2012]. Jos oletetaan, että palvelunestohyökkäysten haittaliikennettä ei rajoiteta lähdepäässä, on hyökkäyksen kohdepäässä oltava ylimäärä kapasiteettia, jotta palvelunesto ei onnistuisi. Kohdepäässä haittaliikennettä voidaan yrittää suodattaa pois tai toisena vaihtoehtona varata käyttöön niin paljon kapasiteettia, että se ylittää haittaliikenteen pois käytöstä viemän kapasiteetin. Molemmissa tapauksissa tarvitaan paljon laitteistotehoa hyökkäykseltä puolustautumiseen. [Chung, 2012]

Chungin [2012] mukaan hajautettujen palvelunestohyökkäysten valmistelu ja hyökkäyksiltä puolustautuminen on kilpailua hyökkääjän ja kohteen välillä, kun molemmat keräävät käyttöönsä lisää kapasiteettia.

Tietoverkkojen takaamisessa ja niiden häirinnässä tunnetaan CIA-periaate, jonka lyhenne tulee sanoista luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Hajautettujen palvelunestohyökkäysten tapauksessa näistä voidaan keskittyä erityisesti saatavuuteen, koska hyökkäykset pyrkivät estämään palvelujen saatavuutta. Toisaalta hajautetuissa hyökkäyksissä käytettyjen bottiverkkojen osalta myös järjestelmien eheys särkyy, kun järjestelmiin murtaudutaan ja ne valjastetaan hyökkäysagenteiksi. [Rauhala ja Hokkanen, 2008]

Rauhalan ja Hokkasen [2008] mukaan saatavuus viittaa siihen, että tietojärjestelmien tarjoamat tiedot ja palvelut ovat niiden käyttöön oikeutettujen asiakkaiden saatavilla maksimaalisen odotusajan sisällä. Mikäli tietyn palvelun osalta näin ei ole, sanotaan palvelun estyneen.

Saatavuutta vastaan kohdistuvat hyökkäykset voidaan jakaa niiden vaikutusten perusteella seuraaviin neljään luokkaan [Rauhala ja Hokkanen, 2008]:

1. esto (deny),
2. tasonlasku (degrade),
3. tuhoaminen (destroy) ja
4. katko (disrupt).

Näistä luokista palvelutasonlasku ja palvelukatko vaikuttavat haittaamalla palvelun käyttöä joko ajallisesti tai kapasiteettia heikentämällä. Palvelun tuhoaminen ja palvelunesto puolestaan tekevät palvelun käyttökelvottomaksi vähintään tilapäisesti.

2.2. Hyökkäyksen vaiheet

Sillberg [2008] jakaa tietoverkkoon tunkeutumisen viiteen vaiheeseen, joiden englanninkieliset nimet alkavat P-kirjaimella. Sillberg viittaa vaiheisiin termillä ”viisi P:tä”:

1. tiedustelu (probe),
2. tunkeutuminen (penetrate),
3. itsepintaisuus (persist),
4. eteneminen (propagate) ja
5. lamauttaminen (paralyze).

Hajautettuja palvelunestohyökkäyksiä toteutettaessa on ensin hankittava pääsy joukkoon kaapattuja verkkolaitteita, botteja, jotka toteuttavat hyökkäyksen käytännössä. Ensimmäinen vaihe on tiedustelu, jossa etsitään verkosta haavoittuvia laitteita kaapattaviksi. Toinen vaihe on laitteisiin tunkeutuminen, jossa esimerkiksi joko salasanan arvaamalla tai tietoturva-aukkoa hyödyntämällä päästään käsiksi kaapattavaan laitteeseen. Kolmannessa vaiheessa hyökkääjä voi tehdä pääkäyttäjän salasanan, joka on vain hänen tiedossaan, tai avata järjestelmään takaportin, jonka kautta laitteeseen on pääsy uudelleen myöhemmin. Neljännessä vaiheessa vallatulta koneelta käsin selvitetään, mitä muuta on saatavilla. Esimerkiksi organisaation sisäverkon muutkin koneet voidaan vallata. Viimeisessä vaiheessa voidaan varastaa tai tuhota tietoa.

Rauhala ja Hokkanen [2008] jakavat palvelunestohyökkäysten valmistelun ja toteutuksen viiteen vaiheeseen:

1. tutkausvaihe,
2. levitysvaihe,
3. tartutusvaihe,
4. kommunikointivaihe ja
5. hyökkäysvaihe.

Tämä luokittelu on tehty erityisesti hajautettujen palvelunestohyökkäysten toiminnan havainnollistamiseksi, joten se eroaa Sillbergin [2008] kuvaamista tunkeutumisen vaiheista. Eri vaiheissa käytetyt tekniikat ovat rakennuspalikoita varsinaisia hyökkäyksiä varten.

Tutkaus voidaan toteuttaa esimerkiksi skannaamalla IP-osoiteavaruutta etsien avoimia portteja verkkolaitteista ja yrittämällä avata yhteys portissa vastaavaan palvelinohjelmaan. IP-osoiteavaruudesta voidaan valita satunnaisia osoitteita, tai voidaan käyttää etukäteen luotua listaa osoitteista [Rauhala ja Hokkanen, 2008]. Portissa vastaava palvelinohjelma saattaa sisältää tietoturva-aukon, jota hyödyntämällä saadaan pääkäyttäjän oikeudet laitteelle. Toinen mahdollisuus on esimerkiksi telnet- tai ssh-palvelinohjelmien käyttäjien – erityisesti pääkäyttäjän – salasanan arvaaminen, jolloin saadaan yhteys laitteen komentotulkkiin.

Kun tutkaus on valmis, voidaan löydetyille laitteille levittää palvelunestohyökkäyksiä toteuttava haittaohjelma, joka on nyt hyökkääjän käytössä ja tottelee häneltä saamiaan komentoja. Tällaisia murrettuja ja käyttöönotettuja laitteita on levitysvaiheen jälkeen hyökkääjän käytettävissä tyypillisesti tuhansia – puhutaan bottiverkosta (botnet).

Bottiverkkoa voidaan ohjata kaapatulta koneelta, joka toimii komentopalvelimena. Hyökkääjän koneen ja komentopalvelimen välillä voi olla ketjussa useita kaapattuja koneita, minkä vuoksi alkuperäisen tekijän jäljittäminen on vaikeaa tai mahdotonta. Lisäksi bottiverkon koneet voivat sijaita fyysisessä maailmassa laajalla alueella – eri maissa ja eri mantereilla – joten tämäkin seikka vaikeuttaa alkuperäisen tekijän jäljittämistä.

3. Hajautetun palveluneston teoriaa

3.1. Internetin tekniikasta

Internetissä käytettävät protokollat ja palvelinsovellukset on suunniteltu sekä pieniä että suuria verkkoja varten: puhutaan skaalautuvuudesta. Internet-protokollaperhettä (Internet protocol suite) käyttävissä verkoissa voidaan välittää tietoa asiakkaalta palvelimelle ja päinvastoin ilman, että sovellusten tarvitsee kiinnittää huomiota esimerkiksi verkon arkkitehtuuriin ja reititykseen. Tiedonsiirron helppous johtaa siihen, että tavallisten verkkosovellusten lisäksi myös haittaohjelmien on helppo käyttää internetiä hyväkseen.

Tämä tutkielma käsittelee hajautettua palvelunestoa, jossa hyökkääjä pyrkii lamauttamaan tietoverkossa tarjolla olevan palvelun käyttäen apunaan useita hyökkäysagentteja. Hyökkäysagentilla (DDoS agent) tarkoitetaan (hajautettuun) palvelunestoon suunniteltua haittaohjelmaa.

Internetin edeltäjä, ARPANET, oli Yhdysvaltain puolustusministeriön luoma verkko, josta muodostui akateemisen maailman yhteydenpitoväline. Sekä ARPANET että nykyinen internet tarjosivat välineet resurssien jakamiseen [ISOC, 2003]. Vuonna 1972 ARPANET-ympäristöön muokatusta sähköpostista tuli nopeasti suosittu sovellus [Zakon, 2003]. Internetin menestykseen onkin vaikuttanut muun muassa yhteisöjen ja yksityishenkilöiden helppo pääsy verkossa jaettuun tietoon. Huomattavaa tässä on se, että palvelunestohyökkäykset sotivat internetin perusperiaatetta – resurssien jakamista – vastaan. Tietoverkko, jonka palveluja ihmiset eivät voi käyttää, on hyödytön.

Verkon resursseja jaetaan käyttäjille useiden erilaisten palvelinsovellusten avulla. Esimerkkejä tärkeistä sovelluksista ovat esimerkiksi WWW- ja DNS-palvelut, jotka ovatkin saaneet osansa palvelunestohyökkäyksistä. Lokakuussa 2002 hyökättiin samanaikaisesti kaikkia internetin juuripalvelimia kohtaan. [Caida, 2002]

Verkkotekniikkaa kuvattaessa verkon eri rakenneosaset jaetaan ns. OSI-mallin (Open Systems Interconnection Reference Model) seitsemälle kerrokselle. Kerrokset kuvaavat tiedonsiirtoprotokollien yhdistelmän yhteistoimintaa internetin verkkoliikenteessä. Kuvassa 1 on esitelty OSI-mallin kerrokset ja niiden datayksiköt.

OSI-kerros	Protokollan datayksikkö
sovelluskerros	data
esitystapakerros	data
istuntokerros	data
kuljetuskerros	segmentti
verkkokerros	paketti
siirtokerros	kehys
fyysinen kerros	bitit

Kuva 1: OSI-mallin kerrokset ja niiden datayksiköt.

Yhdysvaltalainen National Cybersecurity and Communications Integration Center [2014] on toteuttanut palvelunestohyökkäystyyppien luokittelun eri OSI-mallin kerrosten mukaan (ks. kuva 2).

OSI-kerros	Palvelunestotyyppi
sovelluskerros	HTTP GET-pyyntö, HTTP POST
esitystapakerros	viallinen SSL-pyyntö
istuntokerros	kytkinlaitteella toimivan telnet-palvelimen vika
kuljetuskerros	SYN-tulva, Smurf-hyökkäys
verkkokerros	ICMP-tulva
siirtokerros	MAC-tulva
fyysinen kerros	fyysisten verkkolaitteiden vioittaminen

Kuva 2: OSI-mallin kerrosten palvelunestotyypit.

Tarkastelen tässä kuvan 2 mukaisesti eri kerroksille sijoittuvien hyökkäystyyppien periaatteita yllä mainitun lähteen [National Cybersecurity and Communications Integration Center, 2014] sekä toisen lähteen [Viestintävirasto, 2016c] pohjalta.

Alimmalla kerroksella eli fyysisellä kerroksella fyysisten verkkolaitteiden vioittaminen ohjelmallisesti lienee vaikeaa, mutta tämä palvelunestotapa tulee tyypillisesti esiin esimerkiksi kaivinkoneen katkaistessa vahingossa maahan kaivetun valokuidun, jolloin kyseisen kuidun kautta tapahtuva liikenne estyy – estäen samalla valokuidun kautta tavoitettavien palveluiden käyttämisen. Langattomien verkkojen, kuten WLAN- ja 4G-verkkojen, fyysisen kerroksen toimintaa voidaan haitata tai estää haitallista signaalia lähettävällä laitteistolla. Langattomat verkot toimivat radioaalloilla, joten kyseessä on eräänlainen radiohäirintä.

Siirtokerroksen tarkoituksena on muodostaa ja ylläpitää yhteyksiä fyysisen kerroksen yllä. Siirtokerroksessa tapahtuvaa palvelunestoa on MAC-tulva, jossa käytetään hyväksi monien kehittyneiden kytkinten sisältämää maksimimäärää porttiin kytkettyjen laitteiden MAC-osoitteille. Kun kytkimen porttiin lähetetään ohjelmallisesti tulva väitetysti porttiin kytkettyjä MAC-osoitteita, kytkin ei enää ota vastaan liikennettä uusilta laitteilta.

Verkkokerroksessa tapahtuu tietoliikenteen reititys ja kytkentä eri lähiverkkojen tai internetverkkojen välillä. Verkkokerroksen toimintaa voidaan häiritä ICMP-tulvan (Internet Configuration Message Protocol) avulla, jolloin hyökkääjä käyttää ICMP-viestejä ylikuormittamaan kohdeverkon kaistanleveyttä.

Kuljetuskerroksen hyökkäyksiä ovat SYN-tulva ja Smurf-hyökkäys. SYN-tulvassa väärinkäytetään yhteydellisen TCP-protokollan kolmivaihekättelyä, jonka nimensä mukaisesti tulisi normaalisti muodostua kolmesta vaiheesta, mutta palvelunestotarkoituksissa avataan vain ensimmäinen vaihe, TCP-protokollan SYN-yhteydenmuodostuspaketilla ja jätetään kättely viimeistelemättä, jolloin kohdepalvelimen puoliksi muodostuneet yhteydet varaavat resursseja palvelimelta, palo-

muurilta ja muiltakin verkkolaitteilta. Smurf-hyökkäys toteutetaan lähettämällä väärennetyllä lähdeosoitteella varustettuja ICMP-paketteja verkon broadcast-osoitteeseen, jolloin kaikki kyseisen verkon laitteet saavat kyselyn ja mahdolliset vastaukset menevät väärennettyyn, hyökkäyksen kohteena olevaan osoitteeseen.

Istuntokerroksen hyökkäyksissä voidaan käyttää apuna esimerkiksi verkon kytkinlaitteella olevan palvelimen vikoja, jolloin palvelu estyy laitetasolla.

Esitystapakerroksessa hyökkäykset perustuvat viallisiin protokollapyyntöihin, kuten SSL-protokollan väärinkäyttöön.

Sovelluskerroksen palvelunestohyökkäyksissä kyse voi olla HTTP-protokollan GET- tai POST-tulvasta.

3.2. Esineiden internetin tekniikasta

Esineiden internetin turvallisen toiminnan takaamiseksi tarvitaan seuraavat ominaisuudet [Sonar and Upadhay, 2014]:

1. luottamuksellisuus,
2. eheys,
3. saatavuus ja
4. autenttisuus.

Esineiden internetin tietoturvasta on tehty tutkimuksia, joissa luokitellaan erilaisia hyökkäystyyppejä IoT-laitteita vastaan. Yleisesti esineiden internetissä on kolme pääarkkitehtuurikerrosta, jotka ovat verkkokerros, sovelluskerros ja havaintokerros. Jotta IoT-laitteet olisivat turvallisia, useita yksityisyysperiaatteita ja tietoturvaprotokollia on toteutettava jokaiselle näistä kerroksista. [Tabrizi and Ibrahim, 2016]

Tabrizi ja Ibrahim [2016] esittelevät esineiden internetin laitteiden turvallisuushyökkäyksiä hyökkäystyypeittäin. Näitä tyyppejä ovat:

- fyysiset hyökkäykset,
- sivukanavahyökkäykset,
- kryptoanalyysihyökkäykset,
- ohjelmistohyökkäykset ja
- verkkohyökkäykset.

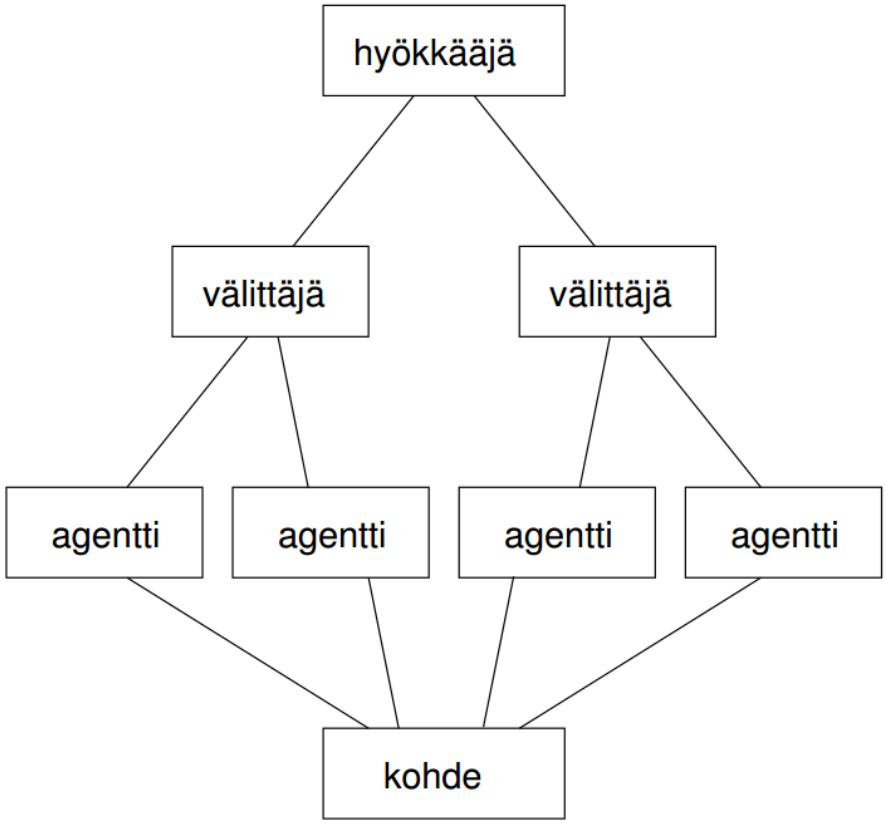
Tässä tutkielmassa tarkastelemme näistä hyökkäystyypeistä erityisesti verkkohyökkäyksiä, joihin palvelunestohyökkäyksetkin kuuluvat. Verkkohyökkäykset jaetaan vielä kahteen luokkaan, jotka ovat aktiiviset hyökkäykset ja passiiviset hyökkäykset. Aktiiviset hyökkäykset pysäyttävät IoT-palvelut suoraan ja passiiviset hyökkäykset tarkkailevat IoT-tietoja haittaamatta palveluja.

Hajautetut palvelunestohyökkäykset ovat yleisin verkkohyökkäysten tyyppi. Nämä hyökkäykset lukeutuvat aktiivisiin hyökkäyksiin, joiden tarkoituksena on estää IoT-palvelu.

3.3. Tyypillisiä palveluneston piirteitä

Hajautetulle palvelunestolle on tyypillistä, että hyökkäys ei tapahdu suoraan hyökkääjän (attacker) koneelta vaan välittäjien (handler) ja agenttien (agent) kautta kohdetta vastaan (kuva 3). Hyökkääjän ja kohteen välissä olevat laitteet ovat murrettuja laitteita, joille hyökkääjä on asentanut käyttämänsä DDoS-työkalut.

Kuvassa 3 esitetty hyökkääjän tietokone ei ole välttämättä hyökkääjän omistama vaan sekin saattaa olla murrettu. Tekijän jäljittäminen on sitä monimutkaisempi prosessi, mitä pidempi ketju murrettuja koneita hyökkääjän ja kohteen välille jää. Palvelunesto ja tietomurrot liittyvät usein läheisesti toisiinsa, koska hyökkääjälle on edullista käyttää murrettujen koneiden sarjaa jälkiensä peittelyyn. Lisäksi murrettuja koneita valjastetaan hyökkäysagenteiksi odottamaan hyökkäyskäskyä.



Kuva 3: DDoS-arkkitehtuuri

Modernit hyökkäykset käyttävät bottiverkkoja (botnet), jossa yksi hyökkääjä ohjaa useita murrettuja tietokoneita hyökkäämään valittuun kohteeseen. Tällöin saavutetaan suuri hyökkäysvoima, kun bottiverkon koneet muodostavat yhteisen hyökkäysaseen kohdetta vastaan. Bottiverkon koneet voivat olla murrettuja tietokoneita tai esineiden internetin laitetta. Hyökkääjälle houkuttavimpia kohteita ovat sellaiset esineiden internetin laitteet, joissa on tunnettu tietoturva-aukko tai joihin on jätetty tehdasasennettu pääkäyttäjän tunnus ja salasana.

3.4. Haavoittuvuuksista

Verkkosovelluksista löytyy jatkuvasti lisää palvelunestolle altistavia haavoittuvuuksia, mutta toisaalta vikoja korjataan ja havaitut ongelmat otetaan entistä paremmin huomioon uusia sovelluksia suunniteltaessa. Avoimen lähdekoodin maailmassa pahantekijöiden on helppo löytää tietoturva-aukkoja hyödynnettäväksi, mutta lähdekoodin julkisuudesta seuraa myös se, että havaitut viat korjataan nopeasti.

Koska DDoS-hyökkäyksiltä suojautumista ei ole otettu huomioon kaikkien verkkosovellusten, -protokollien ja -laitteiden suunnittelussa, niistä löytyy aika ajoin virheitä, jotka altistavat järjestelmän palvelunestolle. Tietoturvakysymykset ovat nousseet esille internetin käyttäjämäärän kasvaessa. Verkkosovellusten turvallisuus perustuu siihen, että kaikki tietoliikenteen osatekijät ovat turvallisia.

Mahdollisia tekniikasta johtuvia haavoittuvuuksia aiheuttavat seuraavat kolme tekijää:

- virheet ohjelmien ja protokollien suunnittelussa,
- virheet ohjelmien ja protokollien toteutuksessa sekä
- virheet järjestelmän ja verkon asetuksissa.

Erilaisia hyökkäystyyppejä ovat [Incapsula, 2017]:

- volyymipohjaiset hyökkäykset,
- protokollahyökkäykset ja
- sovelluskerroksen hyökkäykset.

Esimerkkinä TCP/IP-protokollan alttiudesta palvelunestolle voidaan mainita niin sanottu SYN-hyökkäys, jossa protokollaan kuuluvaa kolmivaiheista kättelyä ei viedä loppuun saakka vaan hyökkäävä asiakaskone lähettää kohdepalvelimelle ainoastaan suuren määrän SYN-paketteja, aloituspyyntöjä. Hyökkäyksen tuloksena kohdepalvelimen aloituspyynnöille tarkoitettu jono täyttyy, jolloin palvelin ei voi avata uusia yhteyksiä ennen kuin jono tyhjenee vanhentuneista pyynnöistä jonkin ajan kuluttua [Hatch and Lee, 2003].

Palvelunestohyökkäys suuntautuu aina tiettyä haavoittuvuutta kohti. Kohde voi olla sovelluksessa oleva aukko. Toisaalta palvelu voidaan estää käyttämällä verkkokaistaa siten, että muille käyttäjille ei jää tilaa.

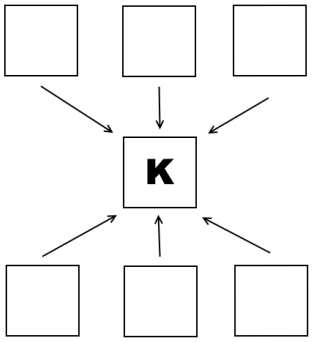
Hyökkäyksiin liittyen voidaan kysyä: ”Mitä tietoturva on?” Tiedon on oltava paitsi tallessa (varmistettu) ja suojassa (salattu), myös oikeiden henkilöiden saatavilla tarvittaessa. Palvelunestohyökkäykset eivät suuntaudu ensisijaisesti tietomurtoihin tai tiedon hävittämiseen, vaan kyseessä on tietoliikenteen häiritseminen ja saatavuuden estäminen. Kuitenkin palvelunestohyökkäysten valmistelussa käytetään usein tietomurtoja bottiverkkojen muodostamiseen.

Viat käyttöjärjestelmän ytimessä voivat altistaa paikalliselle palvelunestolle, mutta hajautetussa palvelunestossa painopiste on suuressa ylivoimassa lukuisten hyökkääjien osallistuessa saman yksittäisen kohteen lamauttamiseen.

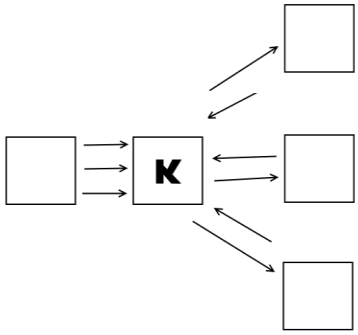
3.5. Hyökkäystyyppien luokittelua

Hajautetut palvelunestohyökkäykset voidaan luokitella teknisen toteutuksensa mukaan kolmeen luokkaan [Fastly, 2016], joita havainnollistavissa kuvissa hyökkäyksen kohde on merkitty K-kirjaimella:

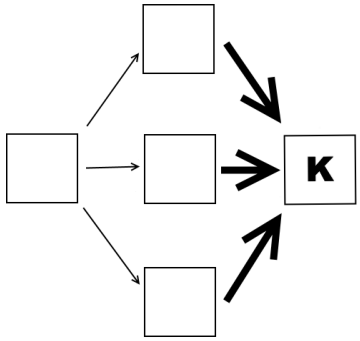
1. tulvahyökkäys (flood), kuva 4,
2. heijastushyökkäys (reflection), kuva 5 ja
3. vahvistushyökkäys (amplification), kuva 6.



Kuva 4: Tulvahyökkäys.



Kuva 5: Heijastushyökkäys.



Kuva 6: Vahvistushyökkäys.

Näistä hyökkäystyypeistä tulva (kuva 4) tarkoittaa useiden hyökkäysagenttien tekemää ylikuormitushyökkäystä, jossa hyökkäysagentit lähettävät kohteeseen enemmän liikennettä kuin se kestää. Tyypillinen tulvahyökkäys hyödyntää TCP-protokollan kolmivaihekättelyä. Hyökkääjä lähettää synkronointipyynnön (SYN) kohdepalvelimelle, joka vastaa synkronointivahvistuksella (SYN-ACK), joka on avoin kutsu yhteyden muodostamiseen. Hyökkääjä jättää synkronointivahvistuksen avoimeksi täyttäen palvelimen avoimien yhteyksien listan tällaisilla valheellisilla pyynnöillä, minkä seurauksena hyökkäyksen kohdepalvelin ei voi vastata uusiin luvallisiin yhteyksiin. [Fastly, 2016]

Heijastushyökkäys (kuva 5) alkaa kyselyllä kohdepalvelimelle, kuten tulvahyökkäys. Hyökkääjän lähettämä alkuperäinen pyyntö lähetetään väärennetyllä lähdeosoitteella. Kun kohdepalvelin vastaa, pyyntö muutetaan ja heijastetaan takaisin kohdepalvelimelle uutena pyyntönä. Nämä heijastetut pyynnöt muodostuvat pian suureksi taakaksi kohdeverkolle. Heijastushyökkäykset eivät vaadi hyökkääjältä yhtä suurta infrastruktuuria – eli käytännössä bottiverkkoa – kuin tulvahyökkäykset. [Fastly, 2016]

Vahvistushyökkäykset (kuva 6) keskittyvät lähettämään ulos näennäisen harmittomia pyyntöjä useille laitteille, olivatpa ne murrettuja tai eivät, ja sitten ohjaamaan kooltaan alkuperäisiä pyyntöjä suuremman vastauksen hyökkäyksen kohdepalvelimelle. [Fastly, 2016]

Fastly [2016] mainitsee, että suurimmat modernit hajautetut palvelunestohyökkäykset käyttävät elementtejä sekä heijastus- että vahvistushyökkäyksistä saadakseen hyökkäyksestä mahdollisimman suuren.

3.6. Yleisiä kohteita hyökkäyksille

Fastly [2016] luettelee yleisimpiä hajautettujen palvelunestohyökkäysten kohteita. Niitä ovat muun muassa seuraavat:

- pelipalvelimet,
- tiedotusvälineiden verkkosivut,
- televiestintäyritykset ja
- taloussektori, kuten pankit ja vakuutuslaitokset.

Toisessa tutkimuksessa [Loukas and Öke, 2010] luetellaan edellä mainittujen lisäksi seuraavat yleiset palvelunestohyökkäysten kohteet:

- sähköisen kaupankäynnin järjestelmät (e-commerce) ja
- valtionhallinnon järjestelmät.

Samoja raportteja laajentaakseni lisään listalle muun muassa seuraavat kohteet:

- esineiden internetin laitteet,
- itseohjaavat autot tulevaisuudessa, kun autot viestivät yhdessä toistensa ja tienvarsien kanssa,
- kiinteistöjen ohjaus- ja hallintajärjestelmät, kuten lämmitysjärjestelmät, sekä
- joukkoliikenteen lipunmyyntijärjestelmät.

4. Suojautumisesta

Hajautetuilta palvelunestohyökkäyksiltä suojautuminen voidaan jakaa kahteen osa-alueeseen [Mirkovic et al., 2004]:

1. hajallaan verkossa olevien laitteiden suojaaminen tietomurroilta ja
2. varsinaisten palvelunestohyökkäysten kohteiden suojautuminen haittaliikenteeltä.

Ensimmäisen kohdan toteuttaminen on kiinni itse kunkin verkosta löytyvän laitteen valmistajasta ja ylläpitäjästä. Valmistajan olisi otettava huomioon laitteen suojaus jo suunnitteluvaiheessa, jotta laitetta ei saataisi murrettua ja liitettyä liian helposti osaksi palvelunestohyökkäyksen bottiverkkoa. Toisen kohdan toteuttaminen riippuu koko tietoverkosta hyökkääjäkoneiden ja hyökkäyksen kohteen välillä. Tässä luvussa käsitellään kahdesta edellä mainitusta kohdasta jälkimmäistä eli hyökkäyksen kohteen puolustuskeinoja.

Mirkovic [2004] käsittelee syitä siihen, miksi hajautetut palvelunestohyökkäykset ovat niin tehokkaita hyökkääjän kannalta ja erittäin vaikeita puolustautua kohteen kannalta. Syitä ovat:

- Yksinkertaisuus. On useita valmiita DDoS-työkaluja, jotka voidaan helposti ladata verkosta ja ottaa käyttöön. Ne tekevät hyökkäyksistä helppoja jopa kokemattomille käyttäjille. Toisaalta tietyt olemassa olevat verkkosovellukset ja -protokollat ovat tekniseltä rakenteeltaan sellaisia, että niiden haavoittuvuuksia voidaan käyttää hyödyksi hyökkäyksissä.
- Liikenteen monimuotoisuus. Hyökkäysliikenteen ja luvallisen liikenteen samankaltaisuus tekee niistä vaikeita erottaa toisistaan ja tällöin esimerkiksi hyökkäysliikenteen suodattaminen pois on vaikeaa.
- IP-osoitteiden väärennys. Osoitteiden väärennys saa hyökkäysliikenteen näyttämään siltä kuin se olisi lähtöisin lukuisilta luvallisilta asiakkailta verkon eri puolilta. Tämä estää suojautumisen sellaisilla menetelmillä, joissa pyritään estämään liikenne mustalle listalle lisätyistä IP-osoitteista.
- Suuri liikenteen volyymi. Volyymipohjaiset hyökkäykset ylikuormittavat kohteen resursseja, mutta tekevät vaikeaksi liikenteen profiloinnin luvalliseen ja luvattomaan. Hyökkäyksiltä puolustautumisen pääongelma on luvallisen ja luvattoman liikenteen erottaminen toisistaan.
- Lukuisat hyökkäysagenttilaitteet. Hajautettujen palvelunestohyökkäysten vahvuus on lukuisten hyökkäysagenttien hajauttaminen ympäri internetiä. Lukuisilla hyökkäysagenteilla hyökkääjä voi estää jopa suurimpien palveluiden toiminnan, koska haittaliikenteen volyymi on niin suuri.
- Internetin topologian heikot pisteet. Nykyisessä internetissä olevassa niin sanotussa hub-and-spoke -topologiassa on kourallinen suureen liikenteeseen varautuneita pisteitä (hub), jotka välittävät liikennettä muualle internetiin. Jos tällaiset pisteet saadaan ylikuormitettua, internet ei ole enää käytettävissä.

Puolustautumismekanismit palvelunestohyökkäyksiä vastaan sisältävät seuraavat elementit [Loukas and Öke, 2010]:

- hyökkäyksen havaitseminen,
- saapuvien pakettien luokittelu sallittuun ja kiellettyyn liikenteeseen sekä
- vaste.

Puolustautuminen hyökkäykseltä vaatii hyökkäyksen havaitsemista, minkä jälkeen monet erilaiset puolustusjärjestelmät luokittelevat saapuvat paketit normaalin tietoliikenteen sallittuihin ja hyökkäysliikenteen kiellettyihin paketteihin. Tämän jälkeen puolustusjärjestelmä vastaa hyökkäykseen esimerkiksi suodattamalla pois liikenteen suodatuspisteessä hyökkäysliikenteen ja päästämällä läpi normaalin liikenteen. [Loukas and Öke, 2010]

Palvelunestohyökkäysten havaitsemiseen on kehitetty useita erilaisia menetelmiä, joista tässä mainitsen vain nimeltä seuraavat kirjallisuudesta löytyvät tyypit [Loukas and Öke, 2010]:

- oppimistekniikat, kuten
  - neuroverkot ja
  - geneettiset algoritmit,
- tilastollinen signaalianalyysi ja
- moniagenttijärjestelmät.

Palveluneston monimuotoisuus ja ongelman vakavuus ovat johtaneet lukuisiin puolustusmekanismeihin. Hajautetuilta palvelunestohyökkäyksiltä suojautuminen vaatii usein monimutkaista liikenteen suodatusta ja verkonhallintakokemusta. Tässä luvussa esiteltävät suojautumistavat voidaan luokitella viiteen ryhmään:

- verkkoliikenteen suodatus,
- kuormantasaus,
- kohdepalvelimien suorituskyvyn lisääminen,
- klusterointi ja
- sisällönvälitysverkkojen (content delivery network, CDN) käyttäminen.

Yksinkertaisin tapa estää internetistä tuleva palvelunestohyökkäys organisaation sisäverkkoon päin on IP-pohjainen suodatus IP-osoitteiden mustanlistan avulla. Raa'alla voimalla (brute force) tehdyt hyökkäykset vaativat melko suuren verkon hyökkääviä isäntäkoneita onnistuakseen estämään suurehkojen www-palvelimien toiminnan. Verkonvalvojat tunnistavat usein tämän tyyppiset hyökkäykset ja ovat taitavia suodattamaan pois sisäverkkoon suuntautuvan haittaliikenteen ennen kohteen ylikuormittumista. [Fastly, 2016]

Hajautetussa palvelunestohyökkäyksessä on kyse tapauksesta, jossa muodostetaan vallatuista järjestelmistä koottu hyökkäysverkko. Eräs hajautettujen palvelunestohyökkäysten ehkäisyyn suunnitelluista tavoista on hyökkäyksen esto lähdepäässä [Mirkovic et al., 2002].

Ehkäisyyn lähdepäässä on kehitetty D-WARD-niminen sovellus, joka tarkkailee kaksisuuntaista liikennettä verkon ja muun internetin välillä sekä tekee säännöllisiä vertailuja havaitun liikenteen ja normaalin tietovirran välillä. Normaalista tietovirrasta poikkeavaa liikennettä rajoitetaan

suhteessa sen aggressiivisuuteen. Ideaalitapauksessa hajautetut palvelunestohyökkäykset estetäänkin niin lähellä lähdepäätä kuin mahdollista.

IP-osoitteiden väärennystä (IP address spoofing) voidaan ehkäistä käyttämällä organisaation sisäverkossa NAT-palvelimen taakse piilotettuja yksityisen verkon IP-osoitteita, jotka on määritelty RFC 1918:ssa. Menetelmä perustuu siihen, että internetin reitittimien pitäisi (RFC:n mukaan) suodattaa liikenteestä paketit, jotka on osoitettu yksityisiin IP-osoitteisiin [Hunt, 2002]. Tämän suojakeinon toimivuus voidaan varmistaa asettamalla oman organisaation palomuuri suodattamaan verkkoliikenteestä ainakin seuraavat poikkeukselliset paketit [Kargl et al., 2001]:

- internetistä tulevat paketit, joiden lähdeosoite viittaa sisäverkkoon ja
- sisäverkosta lähtevät paketit, joiden lähdeosoite viittaa internetiin.

Kuormantasaus tarkoittaa menettelyä, jossa useammalle kuin yhdelle palvelimelle tuleva kuorma jaetaan tasan useiden palvelinten kesken. Kuormantasauksen yksinkertaisin muoto on round robin -menetelmää käyttävän TCP-välityspalvelun (TCP proxy) käyttäminen. Kuormantasauksen yhteydessä round robin tarkoittaa sitä, että saapuvat HTTP-pyynnöt lähetetään järjestelmällisesti yksi kerrallaan peräkkäisille palvelimille.

Pakettien suodattamisen ja kuormantasauksen lisäksi joissakin tapauksissa hajautetulta palvelunestohyökkäykseltä voidaan suojautua lisäämällä kohdepalvelimen suorituskykyä klusteroinnin avulla. Klusteroinnissa saapuvan verkkoliikenteen aiheuttama prosessointikuorma voidaan jakaa palvelimien kesken rakentamalla kahdesta tai useammasta tietokoneesta koostuva klusteri (cluster). Klusterissa käytetään rinnakkaissuoritusta, joka tarkoittaa kaikkien suorittimien valjastamista saman tehtävän pariin.

Palvelunestohyökkäyksiltä voidaan suojautua myös sisällönvälitysverkkojen (content, delivery network, CDN) avulla. Täydessä mittakaavassa palvelukohtainen palvelunestohyökkäyksiltä suojautuminen ei ole kustannustehokasta, joten monet organisaatiot ovat siirtymässä pilvipalveluntarjoajiin suojautuakseen hyökkäyksiltä. Käyttämällä reunapohjaista suodatusta (edge-based filtering), haitallinen liikenne voidaan estää ennen, kun se muodostuu ongelmaksi. Erityisesti sisällönvälitysverkkojen palveluntarjoajat tarjoavat tehokkaan ja skaalautuvan vaihtoehdon niiden vankkojen verkkojen, suuren kapasiteetin ja hajautettujen resurssien ansiosta. [Fastly, 2016]

Sisällönvälitysverkot tarjoavat kaksi muotoa pilvipohjaiselle suojautumiselle [Fastly, 2016]:

1. Aina päällä -ratkaisut, jotka käyttävät rivisuodatusverkkoa (inline scrubbing network) liikenteen tarkkailuun ja epäilyttävän liikenteen poistamiseen reitittämättä erikoistuneiden palvelimien kautta.
2. Tarvittaessa päällä -ratkaisut, jotka keskittyvät uudelleenreitittämään liikennettä verkkopohjaisten suodatuskeskusten (network-based scrubbing center) kautta.

Jotkut sisällönvälitysverkot tarjoavat potentiaalisesti näkyvyyden kaikkeen kaksisuuntaiseen liikenteeseen (salattuun ja salaamattomaan) antaen niille ihanteellisen paikan johdonmukaiseen haittaliikenteen lieventämiseen.

Fastlyn [2016] mukaan viime vuosina on ollut havaittavissa siirtymistä perinteistä tulvahyökkäyksistä heijastus- ja vahvistushyökkäyksiin.

5. Historiaa

Tässä luvussa esittelen palvelunestohyökkäysten ja niihin käytettyjen työkalujen historiaa 1990-luvun loppupuolelta alkaen.

Ensimmäiset palvelunestotyökalut alkoivat ilmestyä vuonna 1998. Ne eivät olleet luonteeltaan aidosti hajautettuja, mutta sallivat hyökkääjän tehdä erilaisia hyökkäyskombinaatioita (TCP-, UDP- ja ICMP-tulvia). Rauhala ja Hokkanen [2008] käyttävät näistä varhaisista työkaluista nimitystä ”palvelunestohyökkäyksien suorittamiseen tarkoitetut pakkaukset”.

Heinäkuussa 1999 alkoivat ilmestyä ensimmäiset varsinaiset hajautetut DDoS-hyökkäystyökalut, kuten Trinoo, TFN ja TFN2K, jotka tarjosivat pakkausten tavoin useita erilaisia hyökkäysmenetelmiä. Nämä työkalut voitiin hajauttaa useille murretuille tietokoneille internetissä, ja niiden hyökkäysagentteja ohjattiin välittäjäohjelmien kautta, mikä vaikeutti alkuperäisten hyökkääjien selvittämistä. Rauhalan ja Hokkasen [2008] mukaan työkalujen syntymäkenttänä olivat IRC-kanavat, joilla hakkeriryhmät kävivät reviiritaistelujaan.

Aluksi hyökkäysagenttien asentaminen vaati manuaalisia tietomurtoja internetissä oleville tietokoneille, mutta prosessin hitaus johti sen automatisointiin. Tällöin saatettiin vallata nopeasti suuri joukko verkkoon kytkettyjä koneita bottiverkoksi. [Rauhala ja Hokkanen, 2008]

Hyökkäysten tekijöistä Rauhala ja Hokkanen [2008] kirjoittavat: ”Vastoin yleistä käsitystä HPE-hyökkäykset eivät ole hienostuneita eliittihakkereiden suorittamia hyökkäyksiä. Nykyään on olemassa suuri valikoima helppokäyttöisiä hyökkäystyökaluja, joiden avulla kuka tahansa, jolla on tietämystä tietokoneista ja tietoverkoista, kykenee suorittamaan vakavan hyökkäyksen.” Kirjoittajat ovat oikeassa siinä, että hyökkäysten tekeminen jossakin mittakaavassa onnistuu monelta tietoteknisesti valistuneelta käyttäjältä, mutta Rauhalan ja Hokkasen julkaisun jälkeen hyökkäysten tekijöissä on ollut siirtymää kohti eliittihakkereita ja järjestelmällisesti johdettuja tahoja, jotka pyrkivät suuriin tuhoihin.

Kuitenkin Kyberturvallisuuskeskuksen Tomi Hasu arvioi [Kähkönen, 2017], että: ”Suurin osa hyökkäyksistä on nettikiusaamista tai ilkivaltaa. Ajattelemattomien nuorten ihmisten kiusantekoa, joka voi kohdistua toisiin nuoriin tai vaikka valtionhallintoon.” Edelleen Hasu kertoo, että valtaosa päivittäisistä hyökkäyksistä on tehty osto- tai vuokrapalveluina. Harvalla on omaa bottiverkkoa käytössä.

Eräs historian suurimmista palvelunestohyökkäyksistä tapahtui lokakuussa 2002, jolloin hyökättiin kaikkia internetin juuripalvelimia kohtaan. Yhdeksän juuripalvelinta yhteensä kolmestatoista oli vaikeassa häiriötilassa. Tämä hyökkäys voidaan luokitella koko internetin kaatamisyritykseksi. [Internet Traffic Report, 2002]

Palvelunestohyökkäyksiä tehtiin myös vuonna 2007 – tällöin internetin juurinimipalvelimia kohtaan sekä useita Suomen suosituimpia WWW-sivustoja vastaan. Yleisradio, Suomi24 ja Eniro olivat tärkeimmät hyökkäyksen kohteet. WWW-sivustot toimivat joko hyvin hitaasti tai eivät ollenkaan. Hyökkäyksessä Yleisradion sivuja vastaan Ylen WWW-palvelin kuormitettiin alas tiedos-

tonjako-ohjelmiston yhteyksillä, joka pohjautui vertaisverkkoon. Yhteyksiä Ylen palvelimelle otettiin yli 100 000 eri IP-osoitteesta hyvin lyhyen ajan sisällä. [CERT-FI, 2007]

Huhtikuussa 2007 hyökättiin lukusia virolaisia pankkeja, yliopistoja ja sanomalehtiä vastaan. Kolmen viikon kuluttua hyökkäykset loppuivat, mutta vasta Viron suljettua kaiken kansainvälisen verkkoliikenteen eristäen maan muusta maailmasta. [International Affairs Review, 2016]

Historiallisista tapauksista muistetaan lisäksi botnet-verkkojen levittäminen internetissä vuonna 2008 ja tätä aiemmin [CERT-FI, 2008]. Botnet-verkkoja muodostetaan mm. palvelunesto-hyökkäysten valmistelua varten. Tällaisista haittaohjelmista kehitetään uusia versioita, jotta virustorjuntaohjelmat eivät havaitsisi niitä.

Syys- ja lokakuussa 2016 tapahtuivat tietoturvabloggari Brian Krebsiä, ranskalaista OVH-hostingia ja Dyn-nimipalvelua vastaan tunnetun palvelunestohistorian suurimmat hyökkäykset. Tuolloin kyseessä oli Mirai-haittaohjelma, joka oli saastuttanut satojatuhansia esineiden internetin laitteita, kuten verkkokameroita, DVD-tallentimia ja modeemeja. Hyökkäysten haittaliikenne oli huippukohdissaan yli terabitin sekunnissa, joten se riitti estämään palvelun suurimmiltakin kohteilta. Erityisen haitallista näissä hyökkäyksissä oli Dyn-nimipalvelun toiminnan estäminen, joka sai kyseistä nimipalvelua käyttävät kohteet pois käytöstä. [Kähkönen, 2017]

Vuoden 2016 lokakuussa hyökättiin Suomen julkishallinnon verkkopalveluita vastaan [Yle, 2016]. Hyökkäys vaikutti sähköisten reseptien välittämiseen ja tunnistuspalveluihin. Kohteita olivat reseptipalvelu Kanta sekä Kelan tunnistuspalvelut Vetuma ja Katso. Aamulehden uutisen mukaan hyökkäyksestä ilmoitettiin Viestintävirastoon, ja rikosilmoitus aiottiin tehdä [Aamulehti, 2016]. Edelleen vuoden 2017 kesäkuussa Alkula [2017] kirjoittaa Aamulehden uutisartikkelissa, että häiriöt ovat yhä vaivanneet sähköisten reseptien ja muiden Kanta-palveluiden toimintaa.

Hyökkäykset Kelan palveluita vastaan olivat potentiaalisesti vaarallisia, koska sähköiset reseptit olivat tilapäisesti poissa käytöstä. Aamulehden uutisen mukaan apteekeille oli kuitenkin häiriöiden varalle ohjeet, mikä onkin hyödyllistä kaikkien erilaisten tietotekniikkaongelmien häiritessä Kanta-palvelun tai verkkoliikenteen toimintaa.

6. Tilanne Suomessa

6.1. Valtion tietoturvallisuusohje

Tässä kohdassa käsittelen Valtion tietohallinnon Internet-tietoturvallisuusohjetta [Valtiovarainministeriö, 2003], joka on valtiovarainministeriön antama tietoturvallisuusohje ja laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) toimesta. Ohjeen tarkoituksena on olla apuvälineenä Internet-käytön ja Internetissä tarjottavien palveluiden tietoturvallisen toteutuksen ohjauksessa, suunnittelussa, valvonnassa, itse toteutuksessa ja myös näihin liittyvissä hankinnoissa. Ohje korostaa jatkuvaluonteista ennakoivaa ja ohjeistuksen mukaista tietoteknisen tason tietoturvallisuustyötä.

VAHTI-tietoturvallisuusohje käsittelee palvelunestohyökkäyksiä luvussa ”Internet-verkon ja sen käytön haavoittuvuuksista”. Ohjeen mukaan organisaation sisäisen verkon kannalta internetliittymän kautta tulevat uhkat liittyvät luvattomaan järjestelmään ja verkkoon tunkeutumiseen, verkon kautta kulkeutuviin haittaohjelmiin ja palvelun käytön estymiseen palvelunestohyökkäyksellä tai näiden yhdistelmiin. Ohje myös mainitsee, että organisaation tulee järjestelmällisesti seurata internetin tietoturvauhkia ja kartoittaa niiden vaikutuksia organisaatiolle.

VAHTI-tietoturvallisuusohje huomauttaa edelleen, että palomuurit eivät suojaa palvelunestohyökkäyksiltä, paitsi järjestelmiä, joihin ei päästetä liikennettä palomuurin läpi. Lisäksi ohjeessa mainitaan, että pelkästään palomuurin fyysinen asentaminen ei takaa tietoturvallisuutta, vaan palomuuriin on asennettava suojaava säännöstö.

Koska VAHTI-ohje on suunnattu valtion tietohallinnolle, se näkee palvelunestohyökkäysten pääongelmana sen, että valtion viranomaisten verkossa tarjoama informaatio ja verkkopalvelut estyvät palvelunestohyökkäysten vuoksi. Ohjeen painopiste on kuitenkin enemmän valtionhallinnon verkkopalveluiden tietosisällön oikeellisuuden ja eheyden varmistamisessa. Oikeellisuus voisi olla vaarassa tietomurron yhteydessä, kun hyökkääjä pääsisi muuttamaan verkossa näkyvien dokumenttien asiasisältöä.

VAHTI-ohje on peräisin jo vuodelta 2003, joten sen ikä näkyy palvelunestohyökkäysten aiheuttaminen vaarojen vähäisellä korostuksella. Ohjeen sisältö on edelleen pätevää tietoa, mutta nykyään vastaavanlaiseen dokumenttiin lisättäisiin oletettavasti oma lukunsa palvelunestohyökkäyksistä ja niiltä suojautumisesta.

Nykymuodossaan ohjeen sisällöstä erityisesti palvelunestohyökkäyksiin liittyvät ohjeet järjestelmien käyttöönotosta, valtionhallinnon organisaatioiden verkkotopologioiden suunnittelusta ja palomuurien säännöstöjen suunnittelusta. Lisäksi ohjeessa neuvotaan poistamaan organisaatioiden palvelimilta kaikki tarpeettomat haavoittuvat graafiset käyttöliittymät ja tarpeettomat palvelut.

Tarpeettomien palveluiden poistaminen voi osaltaan ehkäistä murtautumista koneille ja niiden liittämistä osaksi hyökkäyksiin tarkoitettua bottiverkkoa. Tietyissä tapauksissa palveluiden poistaminen palvelimilta voi myös ehkäistä tietokoneiden altistumista kyseisiä palveluita kohtaan suunnatuilta palvelunestohyökkäyksiltä.

6.2. Tilanne vuoden 2016 ulko- ja turvallisuuspoliittisen selonteon mukaan

Hallitus julkaisi kesäkuussa 2016 ulko- ja turvallisuuspoliittisen selonteon, jossa arvioidaan Suomen ulko- ja turvallisuuspoliittista toimintaympäristöä ja esitetään Suomen ulko- ja turvallisuuspoliittiset painopisteet. Selonteon luvussa maailmanlaajuisista kehityssuunnista kirjoittajat lausuvat seuraavaa [Lehto et al., 2017]:

> ”Perinteinen teollistuminen maailmantalouden keskeisenä muutosvoimana on korvautumassa globalisaatiolla ja digitalisaatiolla. Uusien teknologioiden hinnan odotetaan laskevan ja saatavuuden parantuvan pitkälle tulevaisuuteen. Se mahdollistaa näiden teknologioiden integroinnin tavaroiden ja palveluiden tuottamiseen ja murentaa maantieteellisen sijainnin merkitystä.
>
> Globalisaatio jatkuu muun muassa tuotannon automaation, robotiikan, 3D-tulostuksen, digitalisaation, **teollisen internetin** ja keinoälyn varassa kehityssuuntana, jota tavataan kutsua neljänneksi teolliseksi vallankumoukseksi.”

Selonteko siis arvioi uusien teknologioiden integroinnin tavaroiden ja palveluiden tuottamiseen lisääntyvän, ja laskee teollisen internetin eli esineiden internetin erääksi globalisaatiota ja neljättä teollista vallankumousta edistäväksi tekijäksi.

Selonteossa todetaan, että uusilla teknologioilla – kuten esineiden internetillä – on vaikutuksia teollisuus- ja palvelutuotantoon sekä yhteiskuntaan laajemminkin. Arvioiden mukaan neljäs teollinen vallankumous vaikuttaa työpaikkoihin ja verojärjestelmiin, sekä valtioiden kansainväliseen asemaan ja niiden välisiin suhteisiin.

Edelleen selonteko muistuttaa, että kybertoimintaympäristöön liittyvistä kysymyksistä, mukaan lukien digitalisaatio ja kyberturvallisuus, on tullut yhä keskeisempi osa ulko-, turvallisuus- ja puolustuspolitiikkaa. Selonteon mukaan Naton laajennettujen mahdollisuuksien kumppanuusyhteistyö (Enhanced Opportunities Programme) mahdollistaa Suomelle yhteistyön kyberpuolustuksen alalla.

Tulevaisuuden linjauksissa selonteko asettaa Suomen tavoitteiksi maahan kohdistuvan hybridivaikuttamisen tunnistamisen ja kyberturvallisuuden parantamisen. Vuonna 2016 julkaistu selonteko mainitsee, että osana EU:n hybridiuhkien vastaisten toimien kehittämistä Suomi selvittää mahdollisuuksia hybridiuhkiin keskittyvän osaamiskeskuksen perustamiseksi. Myöhemmin vuoden 2017 huhtikuussa valtioneuvoston viestintäosasto tiedotti, että selonteossa mainittu hybridiuhkien osaamiskeskuksen perustamisasiakirja on allekirjoitettu [Valtioneuvosto, 2017].

Valtioneuvoston julkaiseman tiedotteen mukaan osaamiskeskus harjoittaa strategisen tason vuoropuhelua, tutkimusta, koulutusta, konsultointia ja käytännön harjoituksia, joilla pyritään parantamaan valmiuksia hybridiuhkien torjumiseksi [Valtioneuvosto, 2017]. Osaamiskeskus nähdään yhtenä EU:n globaalin strategian osana ja sen tavoitteet nähdään yhtenevinä Naton tavoitteiden kanssa.

Eduskunta julkaisi lokakuun lopussa vuonna 2016 kotisivuillaan hallintovaliokunnan ja puolustusvaliokunnan saamat asiantuntijalausunnot ulko- ja turvallisuuspoliittisesta selonteosta. Tämän tutkielman kannalta erityisen mielenkiintoisia olivat kyberturvallisuuden professorin Jarno Limnéllin [Limnéll, 2016] ja F-Securen asiantuntijan Erka Koivusen [Koivunen, 2016] sekä suojelupoliisin [Suojelupoliisi, 2016] asiantuntijalausunnot.

Suojelupoliisi vastasi asiantuntijalausunnossaan Hallintovaliokunnalle syyskuussa 2016 kyberuhkista määrittelemällä ensin käsitteen seuraavasti:

> ”Kyberuhassa on kyse digitaaliseen ympäristöön kohdistetusta teknisestä hyökkäyksestä, jonka tavoitteena voi olla tiedon anastaminen tai tähän ympäristöön kuuluvan järjestelmän toiminnan häirintä. Koska digitaalisilla järjestelmillä ohjataan reaalimaailman toimintoja, operaation vaikutus voi ilmetä reaalimaailmassa, mutta ensisijainen vaikutus kohdistuu aina silti ensin tietojärjestelmään.”

Edelleen suojelupoliisi arvioi lausunnossaan kyberhyökkäyksen toimivuutta hybridityökaluna:

> ”Kyberhyökkäys ei ole erityisen toimiva hybridityökalu syvän rauhan oloissa, joissa tavoitteena on muovata väestön mielialaa hienovireisesti. Käyttäjä joko ei kyberhyökkäystä havaitse, tai jos havaitseekin, menee hyökkäys normaalin toimistotekniikan toimintahäiriön piikkiin. [--] Kriisiaikana tilanne on kokonaan toinen. Yhteiskuntaa ohjataan digitaalisilla järjestelmillä, jolloin yhteiskunnan toiminnan voi myös lamauttaa digitaalisilla järjestelmillä.”

Teknisistä keinoista suojelupoliisin lausunnossa mainitaan seuraavasti:

> ”Kyberympäristöstä vastaava esimerkki on kriittistä infrastruktuuria ohjaavien järjestelmien ohjelmistoversioiden tietotekninen kartoitus, jota on havaittu useissa Euroopan maissa. Kun vihamielinen valtio tietää kohdeympäristön ohjelmistoversiot, toimivien hyökkäysmenetelmien valitseminen käy kriisitilanteessa nopeasti.”

Lausunnossa mainittu järjestelmien tietotekninen kartoitus on mahdollinen keino myös palvelunestohyökkäyksien valmisteluun. Kartoittamalla voidaan löytää helposti murrettavia kohteita bottiverkkoon lisättäväksi, tai saatetaan löytää palvelinohjelmistoista sellaisia versioita, jotka ovat ohjelmointivirheen vuoksi alttiita hyökkäyksille.

Lausunnon mukaan Suomessa on ollut havaittavissa ilmiöitä, joissa voi olla kyse valmistautumisesta tulevaan vaikuttamiseen, sekä myös suoranaisesta vaikuttamisesta. Konfliktin sattuessa hyökkääjälle voisi olla edullista tehdä palvelunestohyökkäyksiä esimerkiksi tiedotusvälineitä ja valtion kriittisiä palveluita kohtaan.

6.3. Tilanne Suomessa viime vuosina

Suomessa on toteutettu palvelunestohyökkäyksiä 2000-luvulla ainakin seuraavia erityyppisiä kohteita vastaan:

- tiedotusvälineiden verkkosivut,
- Kanta-palvelut: reseptipalvelu, lääketietokanta, potilastiedon arkisto sekä Omakanta,
- kerrostalojen lämmitysjärjestelmät,
- pankit,
- erään presidenttiehdokkaan kampanjasivut, ja
- VR:n lipunmyyntijärjestelmä.

Mediassa eniten julkisuutta ovat saaneet palvelunestohyökkäykset tiedotusvälineiden verkkosivuja vastaan. Tiedotusvälineillä on mahdollisuus tehdä helposti uutisotsikoita tapahtumasta, joka kohdistuu niitä itseään tai toista tiedotusvälinettä kohtaan.

Toukokuussa 2007 hyökättiin useita Suomen suosituimpia WWW-sivuja kohtaan. Tiedotusvälineistä kohteina oli mm. Yleisradio [CERT-FI, 2007]. Syyskuussa 2012 hyökättiin Helsingin Sanomien ja Ilta-Sanomien verkkosivuja vastaan [Uusi Suomi, 2012a; Uusi Suomi, 2012b]. Helsingin Sanomien vastaava päätoimittaja Mikael Pentikäinen vahvisti verkkohyökkäyksen HS.fi:hin. HS.fi oli noin kolme varttia alhaalla syyskuun 2012 hyökkäyksen vuoksi. Joulukuussa 2012 palvelunestohyökkäys kohdistui Uusi Suomi -lehden verkkosivustoa vastaan [Uusi Suomi, 2012c].

Kesäkuussa 2017 palvelunestohyökkäyksen kohteena oli Long Play -verkkomedia [Aamulehti, 2017a]. Taustalla oli ilmeisesti Long Playn pitkä ja tuolloin suurta julkisuutta saanut verkkoartikkeli, jossa paljastettiin poliisien kirjoittaneen rasistisia tekstejä suljetussa Facebook-ryhmässä.

Median lisäksi toinen tärkeä palvelunestohyökkäysten kohde on ollut Kanta-palvelu, joka sisältää reseptipalvelun, lääketietokannan, potilastiedon arkiston, tiedonhallintapalvelun ja Omakanta-palvelun. Kanta-palvelua vastaan on tehty sen toiminta-aikana useita hyökkäyksiä, joista viimeisimpänä hyökkäys kesäkuussa 2017. Palvelunestohyökkäykset ovat voineet vaikuttaa Kanta.fi-, Omakanta- ja Kelain-palveluihin pääsyyn. Lisäksi häiriö on voinut vaikuttaa julkisella internetyhteydellä liittyneisiin reseptin ja potilastiedon arkiston asiakkaisiin. [Aamulehti, 2017b; Kanta, 2017]

Kansalaisten turvallisuuden ja hyvinvoinnin kannalta vaarallisia palvelunestohyökkäyksiä ovat vedenjakelua ja lämmitysjärjestelmiä vastaan tehdyt hyökkäykset. Tällaisia hyökkäyksiä on tehty ainakin marraskuussa 2016. Uutisten mukaan hakkerit häiritsivät tuolloin ainakin kahden kerrostalon lämmitysjärjestelmää palvelunestohyökkäyksellä. Arvioiden mukaan tapauksia oli kuitenkin merkittävästi enemmän, ja vain osa havaittiin. Havaitussa hyökkäyksessä Lappeenrannassa olevia taloja vastaan tehty palvelunestohyökkäys sai kiinteistöjen tietokoneet jumittumaan ja uudelleenkäynnistyskierteeseen, jolloin tietokoneilla hallitut prosessit pysähtyivät ja talojen lämmitys katkesi. [Uusi Suomi, 2016; Tietoviikko, 2016b]

Talouden toimivuutta ja tavallisten ihmisten maksupalveluja vastaan Suomessa on tehty useita palvelunestohyökkäyksiä pankkien järjestelmiin. Esimerkiksi alkuvuodesta 2015 uutisissa rapor-

toitiin hyökkäyksistä Osuuspankkia ja Nordeaa vastaan. Osuuspankin mukaan palvelut toimivat tuolloin, mutta lyhyet katkokset olivat mahdollisia. [Uusi Suomi, 2015]

Palvelunestohyökkäyksillä on myös pyritty vaikuttamaan politiikkaan kohdistamalla hyökkäys presidenttiehdokkaan kotisivuja vastaan. Joulukuussa 2011 hyökättiin erään ehdokkaan sivuja vastaan. Tieto palvelunestohyökkäyksestä tuli kampanjalle viestintävirastolta. Uutisoinnissa enemmän palstatilaa saivat kuitenkin saman ehdokkaan kampanjasivuille avattuun adressiin kirjoitetut törkeydet. [Uusi Suomi, 2011]

Heinäkuussa 2017 tapahtui ulkomailta tullut hyökkäys VR:n lipunmyyntijärjestelmää vastaan [Mannermaa, 2017]. Lipunmyyntijärjestelmä oli poissa käytöstä muutaman tunnin, minkä aikana lippuja ei voinut ostaa verkkokaupasta, lippuautomaateista eikä junien konduktööreiltä.

6.4. Suomessa ja Euroopassa annettuja tuomioita palvelunestosta

Kolme suomalaista alaikäistä henkilöä toteuttivat 2000-luvun alkuvuosina itse haittaohjelman, jolla pystyi suorittamaan palvelunestohyökkäyksiä, ja levittivät ohjelmaa Internetin käyttäjille. Tuusulan käräjäoikeus antoi asiasta tuomion vuonna 2009. Tuomiolauselmassa syyksi luettuja rikoksia olivat: vaaran aiheuttaminen tietojenkäsittelylle, väärennys, luvaton käyttö, tietoliikenteen häirintä, tietomurto ja tekijänoikeusrikos. Rangaistusseuraamuksia olivat 50 päiväsakkoa, vahingonkorvaukset, 40-45 päivää ehdollista vankeutta eri tekijöille ja rikoksentekovälineiden menettäminen valtiolle.

Tivi-lehti kertoo, että Suomessa verkkohäirintätapaukset tutkii yleensä keskusrikospoliisi ja viime vuosina poliisin tietoon on tullut erityisesti valtionhallinnon verkkopalveluita kohtaan tehtyjä palvelunestohyökkäyksiä. Tuomioita Suomessa on kuitenkin annettu harvakseltaan: tietoliikenteen häirinnästä annettiin vuonna 2015 vain kolme tuomiota ja edellisvuonna kymmenen. [Kähkönen, 2017]

Saman Tivi-lehtiartikkelin mukaan Europol ja useiden maiden poliisiviranomaiset tekivät yhteisoperaatiossa vuoden 2016 joulukuussa 34 pidätystä, jotka kohdistuivat alle 20-vuotiaisiin DDoS-vuokrapalveluiden käyttäjiin. Lehti arvioi, että operaatiolla voi olla pelotevaikutus, mutta iskujen määrään sillä tuskin on vaikutusta. [Kähkönen, 2017]

6.5. Skenaarioita rikollisiin ja terroristihyökkäyksiin esineiden internetin avulla

Internetin käyttö rikollisiin tarkoituksiin on jo vanha ilmiö, mutta esineiden internetin myötä mahdollisuudet erilaisiin laittomuuksiin laajenevat. Tzezanan [2016] mukaan voimme odottaa ennestään tuttujen ilmiöiden – kuten kiristysohjelmien, viruksien, vakoiluohjelmien – laajentavan reviiriään myös esineiden internetiin.

Koska esineiden internet laajenee kaikenlaisiin älylaitteisiin kiinteistöautomaatiosta kodinkoneisiin ja viihde-elektroniikkaan, mahdollisten tietomurtojen ja palvelunestohyökkäysten määrään on odotettavissa kasvua. Pilvipohjaisten laitteiden tietomurrot ovat jatkuvassa nousussa – lähteen mukaan murrot lisääntyivät 152 prosenttia vuodesta 2014 vuoteen 2015. Tämä viittaa esineiden

internetin laitteiden, kuten esimerkiksi puettavien laitteiden, älykkäiden valaistusjärjestelmien ja yritysympäristön sulautettujen antureiden hakkerointiin. [Wong, 2016]

Kodin viihde-elektroniikan käyttämistä ihmisten vakoiluun ja henkilökohtaisten tietojen anastamiseen on jo tapahtunut. Monet tietoturvastaan huolestuneet ihmiset ovat jo ottaneet tavakseen peittää esimerkiksi kannettavan tietokoneen, taulutietokoneen tai älytelevision kameran läpinäkymättömällä teipillä, jotta mahdollisen tietomurron onnistuttua laitteen kamera ei voisi välittää kuvaa murtautujalle.

Esineiden internet on erityisellä vaaravyöhykkeellä, koska se on uusi teknologia, jonka väärinkäyttö on vasta alkuvaiheessaan. Perinteiset tietotekniset laitteet ovat jo usein suojattuja virustorjuntaohjelmistolla ja palomuurilla, mutta moniinkaan esineiden internetin laitteisiin ei tällaisia ohjelmistoja voi asentaa.

7. Palveluneston tutkimusta ja kohteita hyökkäyksille

7.1. Tutkimukseen käytettäviä sovelluksia

Tässä kohdassa esittelen työkaluja palvelunestohyökkäyksien tutkimiseen ja kohteita hyökkäyksille. Painopiste on yleisesti tunnetuissa sovelluksissa ja verkkopalveluissa.

Verkkoliikenteen – ja siten myös palveluneston – tutkimiseen on kehitetty WWW-palvelu nimeltä Emulab (http://www.emulab.net/). Kyseessä on sovellus, jonka avulla on mahdollista luoda fyysinen tietoverkko, jossa verkkoliikennettä voi tutkia emuloidussa ympäristössä. Verkkoliikenteen emulointi tarkoittaa tässä yhteydessä sitä, että verkkoliikenne tapahtuu oikeita tietokoneita ja oikeita verkkokomponentteja käyttäen. Kyse ei siis ole simulaatiosta, joka tapahtuisi tietokoneen muistissa näennäisesti toimivien laitteiden avulla.

Emulabin avulla verkkotopologian voi suunnitella graafisesti ja tietokoneille on mahdollista asentaa vapaavalintainen käyttöjärjestelmä sekä sovellusohjelmat. Näin luotua tietoverkkoa voi käyttää haluamallaan tavalla verkkoliikenteen tutkimiseen. Emulabin avulla voidaan kehittää ja arvioida tietoverkkojen toimintaa sekä etsiä ja korjata potentiaalisia virheitä verkkosovellusten toiminnasta.

The Network Simulator (http://www.isi.edu/nsnam/ns/), joka tunnetaan myös nimellä ns-2, on diskreettien tapahtumien simulaattori, joka on tarkoitettu verkkotutkimukseen. Ns-2 simuloi sille annettujen ohjeiden mukaan monenlaisia IP-verkkoja paketti kerrallaan. Ohjelmalle voidaan antaa malli verkkokonfiguraatiosta, joka kuvaa simuloitavan verkon kaikkia piirteitä, kuten verkon solmujen välisien linkkien kaistanleveyttä ja viivettä.

Ns-2:lla simuloitu verkko voidaan määrittää käyttämään haluttuja verkkoprotokollia, kuten TCP, UDP tai FTP. Verkon solmuissa olevat laitteet voidaan määrittää lähettämään määrätyn kokoisia paketteja verkkoon tietyllä nopeudella. Simulaatiosta voidaan myös tuottaa graafinen animaatio työkalulla, jonka nimi on NAM (Network Animator).

Toinen tässä esittelemäni palvelunestohyökkäysten tutkimiseen soveltuva ohjelma – Low Orbit Ion Cannon (https://sourceforge.net/projects/loic/) – on verkon rasitustestisovellus, jonka avulla voidaan testata verkkopalvelun toimivuutta kuorman alla. LOIC suorittaa tulvamuotoisen palvelunestohyökkäyksen kohdepalvelinta vastaan TCP- ja UDP-paketeilla.

Edellä mainitun Low Orbit Ion Cannon -sovelluksen suunnitteluratkaisujen pohjalta on kehitetty High Orbit Ion Cannon (https://sourceforge.net/projects/high-orbit-ion-cannon/), joka pystyy hyökkäämään internetissä samanaikaisesti jopa 256 URL-osoitetta vastaan. HOIC lähettää annettuihin kohteisiin tulvimalla HTTP-protokollan POST- ja GET-pyyntöjä.

7.2. Esineiden internet hyökkäysten kohteena ja lähteenä

Esineiden internet muodostuu lukuisista ympäri maailmanlaajuista verkkoa sijoitetuista älykkäistä laitteista, joiden tietoturvasta on huolehdittu vaihtelevalla tavalla. Kun internetiin kytkettyjä laitteita on paljon ja kaikilla on oma IPv6-osoite, ne kaikki ovat periaatteessa alttiita palvelunestohyökkäyksille.

Älykkäitä laitteita on teollisuuden lisäksi kotitalouksissa, joissa laitteet saattavat olla esimerkiksi viihde-elektroniikkaa (mm. älytelevisiot) tai kodinkoneita (mm. älyjääkaapit). Älylaitteet voivat olla kiinni internetissä kotireitittimen kautta kiinteällä langallisella verkkoyhteydellä tai langattomasti. Laitteissa voi joskus olla internet-yhteys myös mobiilipuhelinverkon kautta, jolloin laite on varustettu SIM-korttipaikalla.

Koska esineiden internetin laitteissa on koetun historian perusteella ollut runsaasti haavoittuvuuksia, ne ovat olleet houkuttelevia kohteita tietomurroille ja niiden valjastamiselle hyökkäysagenteiksi. Ensimmäisessä vaiheessa laitteen käyttöjärjestelmä otetaan haltuun haavoittuvuuden avulla ja toisessa vaiheessa murrettua laitetta käytetään osana suurta murrettujen laitteiden joukkoa hajautettuihin palvelunestohyökkäyksiin tiettyä verkossa sijaitsevaa kohdetta vastaan.

Tivi-verkkolehden artikkelissa arvioidaan, että erityisesti esineiden internetin ympäristöjen ulkoreunat ovat lähes loputon mahdollisuus tietoturvaa vastaan tehdyille hyökkäyksille. Esineiden internetin verkkojen suojaaminen teettää paljon työtä, koska tarkistettavia laitteita ja rajapintoja on niin runsaasti. Kuitenkin suurimmaksi yritysten ja organisaatioiden tietoturvaongelmien lähteeksi arvioidaan loppukäyttäjät. [Pervilä, 2016]

Tivin artikkelissa esineiden internetiä verrataan pyramidiin, jossa huipulla ovat paljon laskentavoimaa sisältävät laitteet, kuten sylimikrot ja älypuhelimet. Keskellä on rajoitettujen ominaisuuksien laitteita, kuten termostaatteja, tv-laitteita, jääkaappeja ja niin edelleen. Pyramidin pohjan muodostavat dataa keräävät laitteet, anturit, joista monet ihmiset eivät ole kuulleetkaan. Artikkelin mukaan pyramidin huippu on hyvin suojattu laitevalmistajien ansiosta, mutta ongelmat sijaitsevat kahdella alimmalla tasolla. [Pervilä, 2016]

Jo muutamia vuosia sitten tunnettiin kiristyshaittaohjelmia (engl. ransomware), jotka saattoivat esimerkiksi salata tietokoneen kiintolevyn sisällön ja vaatia sen jälkeen lunnaita salauksen purkamista varten. Uutena ilmiönä tunnetaan esineiden internetin kiristysohjelmat (ransomware of things, RoT), jotka estävät tiettyjen esineiden internetin laitteiden toiminnan ja vaativat lunnaita toiminnan palauttamiseksi. Riippuen laitteesta, esineiden internetin laitteen toiminnan estäminen voi olla hyvinkin vakava ongelma.

7.3. Itseohjaavat autot

Älykkäät, itseohjaavat autot ovat pitkään olleet puheenaiheena muun muassa Googlen kehittäessä tekniikkaa, jolla autonkuljettaja voidaan korjata tietotekniikalla. Google aloitti itseohjaavien autojen projektinsa vuonna 2009, minkä jälkeen projektin autot ovat ajaneet yli 1,5 miljoonaa mailia. Tekniikaltaan autot ovat olleet sekä muokattuja tavallisia autoja, että uusia prototyyppiautoja, jotka on suunniteltu projektin piirissä kokonaan itse. [Google, 2016a]

Google perustelee tällaisten autojen kehittämistä turvallisuudella – itseohjaavat autot osaisivat tunnistaa kameratekniikalla ympäriltään kohteita, kuten jalankulkijoita, pyöräilijöitä ja muita autoja. Tällaiset autot käyttäisivät sekä karttatietoja että anturitietoja muodostaakseen käsityksen omas-

ta ympäristöstään. Kohteet tunnistettaisiin koon, muodon ja liikkumiskaavan mukaan. [Google, 2016b]

Googlen autoprojektissa ohjelmisto ennustaa, mitä autoa ympäröivät kohteet saattaisivat tehdä seuraavaksi, kuten esimerkiksi jalkakäytävän reunalla oleva jalankulkija saattaisi ylittää tien auton edessä.

Älykkään liikennetekniikan ja itseohjaavien autojen toivotaan vähentävän liikenneonnettomuuksissa kuolleiden ja loukkaantuneiden ihmisten määrää. Vuoden 2004 tietojen mukaan Euroopan unionin alueella kuoli joka vuosi 40000 ihmistä ja loukkaantui vakavasti 1,7 miljoonaa ihmistä. Lisäksi liikenteen haitoiksi voidaan laskea liikenneruuhkat ja ilmansaasteet, joita liikenne aiheuttaa. [Hubaux et al., 2004]

Perinteisesti liikenteen turvallisuutta on parannettu auton sisäisiä ominaisuuksia kehittämällä, kuten lisäämällä turvavyöt, turvatyynyt ja lukkiutumattomat jarrut. Näitä keinoja tehokkaammaksi turvakeinoksi on arvioitu älykäs liikennetekniikka, jossa autot kommunikoivat keskenään ja yhdessä tienvarsien kanssa. Lokakuussa 1999 Yhdysvalloissa myönnettiin 75 megahertsin taajuuskaista lyhyen etäisyyden kommunikaatioon autosta autoon tai autosta tienvarteen. Tulevaisuuden liikennetekniikka perustunee vahvasti lyhyen kantaman tietoliikenteeseen teillä. [Hubaux et al., 2004]

Itseohjaavien autojen turvallisuutta saattavat heikentää mahdolliset hyökkäykset tekniikkaa vastaan. Palvelunestohyökkäykset voisivat jumittaa liikenteen autosta autoon tai autosta tienvarteen. Hubauxin [2004] artikkelissa arvioidaan, että palvelunestohyökkäyksiin ei ole pelkästään teknistä ratkaisua, joka poistaisi ongelmat, mikä on syy siihen, että tuolloin arvioitiin itseohjaavien autojen olevan kauempana kuin aivan lähitulevaisuudessa.

Verkkouutisten artikkelin [Rydman, 2016] mukaan Euroopan parlamentti on laatimassa sääntöjä roboteille, niiden valmistajille ja käyttäjille. Mietinnössä otetaan kantaa myös itseohjaaviin autoihin. Keskeinen kysymys on, kenen pitää korvata vahingot, jos itseohjaava auto ajaa kolarin. Onko korvaava henkilö auton ohjelmoija, omistaja vai mahdollinen matkustaja?

Iltalehden verkkouutisessa [Iltalehti, 2016] F-Secure-tietoturvayhtiön tutkimusjohtaja Mikko Hyppönen kertoo, että itseajava auto voi synnyttää uudentyyppistä rikollisuutta. Uutisessa spekuloidaan, että saattaisi olla mahdollista varastaa itseohjaava auto murtautumalla etäyhteyden kautta autoon, kun auto on parkkipaikalla odottamassa oikeaa omistajaansa. Siinä vaiheessa, kun itseohjaavat autot ovat osa teollista internetiä ja ne viestivät yhdessä tienvarsien kanssa, voisi olla mahdollista, että joko auto hyökkää palvelunestohyökkäyksellä tienvarsia vastaan tai useat tiellä olevat autot hyökkäävät yksittäistä liikkuvaa autoa vastaan.

8. Yhteenveto

Internetin normaalia toimintaa häiritään useilla erilaisilla haittaohjelmilla, joista palvelunestoon käytettävät sovellukset ovat vain yksi esimerkki. Hajautettujen palvelunestohyökkäystapausten yleistyttyä internetissä on verkkosovellusten sisältämiä palvelunestolle altistavia virheitä korjattu, jolloin ohjelmien laatu on parantunut.

Verkkosovellusten haavoittuvuus hajautetuille palvelunestohyökkäyksille johtuu suunnittelu-, toteutus- ja konfigurointivirheistä, joita havaitaan aika ajoin. Lisäksi eräät verkkoprotokollien suunnitteluratkaisut mahdollistavat tietyntyyppisten palvelunestohyökkäysten toteuttamisen.

Suuren organisaation sisäverkon turvallinen ylläpitäminen vaatii huolellisuutta sekä jatkuvaa työtä turvallisuuden eteen. Eräs yksinkertainen tapa huolehtia internetiin kytketyn verkon turvallisuudesta sekä palvelunestohyökkäyksiä että muita haavoittuvuuksia vastaan on tarpeettomien palvelinsovellusten poistaminen ja sovellusten päivittäminen uusimpiin vakaisiin versioihin säännöllisesti.

Haavoittuvien älylaitteiden määrän lisääntyminen on johtanut siihen, että niitä on helppo murtaa ja valjastaa hyökkäysagenteiksi. Johdantoluvussa käsittelin ennätysmäistä esineiden internetin laitteilla toteutettua palvelunestohyökkäystä, joka tuotti haittaliikennettä jopa 1,1 teratavua sekunnissa. Normaalisti toimiessaan erilaiset älylaitteet voivat olla hyödyllisiä tai viihdyttäviä, mutta murrettuina niiden käyttäminen palvelunestohyökkäyksiin aiheuttaa uuden mittaluokan ongelmia.

Joissakin tapauksissa perinteiset fyysisen maailman palvelut on siirretty verkkoon lähes kokonaisuudessaan. Tästä esimerkkinä mainitsin johdantoluvussa kotimaisen pankin, joka ei tarjoa lainkaan mahdollisuutta laskujen maksamiseen pankin toimipaikassa. Pelkästään verkossa toimivalle palvelulle olisi syytä järjestää varajärjestelmä. Esimerkiksi paperisten reseptien määrääminen toimii varajärjestelmänä sähköiselle Kanta-reseptipalvelulle.

Perinteisen fyysisessä maailmassa toimivan palvelun, kuten vaalien äänestysjärjestelmän, siirtämistä digitaaliseksi kannattaa harkita riittävän pitkään ennen toteuttamista. Verkossa toimiva äänestysjärjestelmä on altis palvelunestohyökkäyksille. Lisäksi äänestäjien henkilökohtaisten tietokoneiden tietoturva on vaihtelevalla tasolla, mikä saattaa aiheuttaa vaaran äänestyksen toimivuudelle ja luotettavuudelle.

Kuten tutkielman kohdassa 6.3 kirjoitin, Suomessa on viime vuosina hyökätty useita erityyppisiä järjestelmiä vastaan. Näistä hyökkäyksistä kerrostalon lämmitysjärjestelmän toiminnan estäminen oli talviaikaan tapahtuneena tekona potentiaalisesti vaarallinen ihmisille. Toisaalta Kelan Kanta-palveluja ja pankkipalveluja vastaan hyökkääminen on omiaan estämään yhteiskunnan normaalia toimintaa.

Käyttöjärjestelmien ja sovellusohjelmien tietoturvaongelmista tiedottavat postituslistat ja sivustot, kuten Viestintäviraston kyberturvallisuusvaroituslista [Viestintävirasto, 2016a] ja haavoittuvuuslista [Viestintävirasto, 2016b] ovat hyödyllistä luettavaa verkon ylläpitäjälle. Ylläpitäjien olisi myös syytä suunnitella erilaisia vaihtoehtoisia toimintatapoja häiriötilanteiden varalle mahdolli-

suuksien mukaan. Kuitenkin jotkin palvelut toimivat vain verkon välityksellä internetissä, joten niiden häiriötilanteen varalle on vaikea suunnitella vaihtoehtoisia järjestelmiä.

Esineiden internet tulee laajenemaan nopeasti jo lähitulevaisuudessa, kun erilaisia verkkoon kytkettäviä laitteita ilmestyy markkinoille. Laitteiden saattaminen nopeasti markkinoille voi olla houkuttelevaa, mutta altistaa ne erilaisille tietoturvaongelmille. Huonosti suojattujen esineiden internetin laitteiden käyttäminen hajautetun palvelunestohyökkäyksen bottiverkossa on jo nykyaikaa. Laitteiden suuri määrä tekee palvelunestohyökkäyksistä aivan uuden mittaluokan ongelman.

Viiteluettelo

[Aamulehti, 2016] Aamulehti, 15.10.2016, s. A17.

[Aamulehti, 2017a] Aamulehden verkkoartikkeli *Palvelunestohyökkäys ilmeisesti Long Playn hidastelun takana, kertoo verkkojulkaisu Twitterissä – Professori tutkisi kirjoittelun*. Saatavilla sähköisesti: https://www.aamulehti.fi/kotimaa/palvelunestohyokkays-ilmeisesti-long-playn-hidastelun-takana-kertoo-verkkojulkaisu-twitterissa-professori-tutkisi-kirjoittelun-200183897/ (viitattu 26.6.2017).

[Aamulehti, 2017b] Aamulehden verkkoartikkeli *Palvelunestohyökkäys haittaa taas Kelan Kanta-palveluita - sähköisessä reseptissä voi olla ongelmia*. Saatavilla sähköisesti: https://www.aamulehti.fi/kotimaa/palvelunestohyokkays-haittaa-taas-kelan-kanta-palveluita-200183678/ (viitattu 26.6.2017).

[Alkula, 2017] Maarit Alkula, Häiriöt halvaannuttavat apteekit. *Aamulehti*, 3.6.2017, s. A9.

[Caida, 2002] Nameserver DoS Attack October 2002, http://www.caida.org/projects/dns/dns-root-gtld/oct02dos.xml (checked 2.3.2017).

[CERT-FI, 2007] *CERT-FI vuosikatsaus 2007*. Saatavilla sähköisesti http://www.cert.fi/katsaukset/2007/vuosikatsaus2007.html (viitattu 5.2.2012).

[CERT-FI, 2008] *CERT-FI vuosikatsaus 2008*. Saatavilla sähköisesti http://www.cert.fi/katsaukset/2008/vuosikatsaus2008.html (viitattu 5.2.2012).

[Chung, 2012] Yoo Chung, Distributed Denial of Service is a Scalability Problem. *ACM SIGCOMM Computer Communication Review* 42, 1 (January 2012), 69-71.

[Fastly, 2016] Fastly.com, *What to Look for When Choosing a CDN for DDoS Protection*. https://www.fastly.com/sites/default/files/Fastly-Bizety%20DDoS%20White%20Paper.pdf (checked 11.10.2016).

[Google, 2016a] *Google Self-Driving Car Project – Where We've been*, https://www.google.com/selfdrivingcar/where/ (checked 12.10.2016).

[Google, 2016b] *Google Self-Driving Car Project*, https://www.google.com/selfdrivingcar/ (checked 12.10.2016).

[Hatch and Lee, 2003] Brian Hatch and James Lee. *Hacking Linux Exposed*. McGraw-Hill, second edition, 2003.

[HS, 2016] Helsingin Sanomat, *Sähköinen äänestys olisi altis ulkopuolisille hyökkäyksille*. Pääkirjoitus 2.10.2016. Saatavilla sähköisesti: http://www.hs.fi/paakirjoitukset/a1475290790315?jako=e9ed16443f756d98ec242e03f40a31c0&ref=tw-share (viitattu 2.10.2016).

[Hubaux et al., 2004] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo, The Security and Privacy of Smart Vehicles. *IEEE Security & Privacy Magazine*, 2004.

[Hunt, 2002] Craig Hunt. *Linux Network Servers*. Sybex, 2002.

[Incapsula, 2017] Incapsula. *DDoS Attacks*. https://www.incapsula.com/ddos/ddos-attacks/ (checked 2.3.2017).

[Iltalehti, 2016] Iltalehden verkkoartikkeli: *Itseajava auto voi synnyttää uudentyyppistä rikollisuutta*. Saatavilla sähköisesti: http://www.iltalehti.fi/autot/2016102522515467_au.shtml (viitattu 17.7.2017).

[Iltasanomat, 2016] Iltasanomien verkkouutinen 25.10.2016, *Hurjalla verkkohyökkäyksellä ihmeellinen tausta: ”Hän julkaisi koodin peittääkseen jälkensä”*. Saatavilla sähköisesti: http://www.iltasanomat.fi/digitoday/tietoturva/art-2000001938417.html?ref=rss (viitattu 25.10.2016).

[International Affairs Review, 2016] *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security*. http://www.iar-gwu.org/node/65 (checked 16.10.2016).

[Internet Traffic Report, 2002] Internet Traffic Report, Backbone DDoS, 2002. http://www.internettrafficreport.com/event/2.htm (checked 16.10.2016).

[ISOC, 2003] Internet Society ISOC. *A brief history of the internet*, 2003. http://www.isoc.org/internet/history/brief.shtml (checked 15.9.2016).

[Jing et al., 2014] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, Security of the Internet of Things: perspectives and challenges. *Wireless Networks* 20, 2014.

[Kallio, 2016] Henripekka Kallio, Valtio luopuu pian paperikirjeistä. *Aamulehti*, 9.11.2016, s. A15.

[Kanta, 2017] Kanta-palvelun häiriötiedote 3.6.2017. Saatavilla sähköisesti: http://www.kanta.fi/fi/hairiotiedotteet/-/asset_publisher/qY011gOk8ZM3/content/kanta-palveluissa-on-esiintynyt-palveluiden-kayttoon-vaikuttavia-palvelunestohyokkayksia-2-3-6-2017-hairio-on-paattynyt-ja-palvelut-toimivat-normaalis (viitattu 26.6.2017).

[Kargl et al., 2001] Frank Kargl, Joern Maier, and Michael Weber. Protecting web servers from distributed denial of service attacks. *Proc. of the 10th International Conference on World Wide Web*, 514-524, 2001.

[Karhumäki et al., 2008] Juhani Karhumäki, Arto Lepistö, Tommi Meskanen, Sami Mäkelä, Hannu Nurmi, Tommi Penttinen, Ari Renvall, Petri Salmela ja Seppo Virtanen. *Auditointiraportti kunnallisvaalien sähköisen äänestyksen pilotista*. Turku Centre Computer Science, TUCS National Publication, No 15, October 2008. Saatavilla sähköisesti: https://www.doria.fi/bitstream/handle/10024/44891/tucspublication15.pdf?sequence=1 (viitattu 27.10.2016).

[Koivunen, 2016] Erka Koivusen asiantuntijalausunto ulko- ja turvallisuuspoliittiseen selontekoon. Saatavilla sähköisesti: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2016-AK-77923.pdf (viitattu 2.11.2016).

[Krebs, 2016a] Brian Krebsin Twitter-viesti 1.10.2016. https://twitter.com/briankrebs/status/782273183974100992 (checked 2.10.2016).

[Krebs, 2016b] Brian Krebs, *Source Code for IoT Botnet "Mirai" Released*. https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/ (checked 2.10.2016).

[Kähkönen, 2017] Heidi Kähkönen, Internetin pommitus pahenee. *Tietoviikko*, helmikuu 2017.

[Lehto et al., 2017] Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi, Mirva Salminen: Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0 (viitattu 22.6.2017).

[Limnéll, 2016] Jarmo Limnéllin asiantuntijalausunto ulko- ja turvallisuuspoliittiseen selontekoon. Saatavilla sähköisesti: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2016-AK-74292.pdf (viitattu 2.11.2016).

[Loukas and Öke, 2010] Georgios Loukas and Gülay Öke, Protection against Denial of Service Attacks: A Survey. *The Computer Journal* 53 (7), 2009, 1020-1037.

[Mannermaa, 2017] Jaakko Mannermaa, VR: Hyökkäys ulkomailta hyydytti lipunmyynnin muutamaksi tunniksi. Yle.fi, 8.7.2017. Saatavilla sähköisesti: https://yle.fi/uutiset/3-9713089 (viitattu 8.7.2017).

[Mirkovic et al., 2002] Jelena Mirkovic, Gregory Prier and Peter Reiher, Attacking DDoS at the Source. *Proc. of the 10th IEEE International Conference on Network Protocols*, 312-321, 2002.

[Mirkovic et al., 2004] Jelena Mirkovic, Sven Dietrich, David Dittrich and Peter Reiher, *Internet Denial of Service: Attack and Defense Mechanisms*. Prentice Hall, 2004.

[National Cybersecurity and Communications Integration Center, 2014] DDoS Quick Guide, DDoS Quick Guide, 2014. https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf (checked 2.3.2017).

[Pervilä, 2016] Markku Pervilä, Teollinen internet uhkaa ajaa tietoturvan polvilleen, 2016. Saatavilla sähköisesti: http://www.tivi.fi/CIO/teollinen-internet-uhkaa-ajaa-tietoturvan-polvilleen-6560153 (viitattu 13.7.2017).

[Pulliainen, 2016] Mikko Pulliainen, Isot nettihyökkäykset entistä isompia. *Aamulehti*, 31.10.2016, s. A16.

[Pulliainen, 2017] Mikko Pulliainen, Verkkohyökkäykset voimistuvat. *Aamulehti*, 1.2.2017, s. A10.

[Rauhala ja Hokkanen, 2008] Olli Rauhala ja Lauri Hokkanen, *Hajautetun palveluneston ja tunkeutumisen torjunta*. Pro gradu -tutkielma, Tampereen yliopisto, Tietojenkäsittelytieteiden laitos, 2008.

[Sillberg, 2008] Risto Sillberg, *Tietoverkkoon tunkeutumisen havaitseminen Snortin avulla*. Opinnäytetyö, Satakunnan ammattikorkeakoulu, 2008.

[Sonar and Upadhay, 2014] Krushang Sonar and Hardik Upadhay, A Survey: DDOS Attack on Internet of Things. *International Journal of Engineering Research and Development*, 10, 11 (November 2014), 58–63.

[Suojelupoliisi, 2016] Suojelupoliisin asiantuntijalausunto ulko- ja turvallisuuspoliittiseen selontekoon. Saatavilla sähköisesti: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2016-AK-77701.pdf (viitattu 2.11.2016).

[Tabrizi and Ibrahim, 2016] Sahar S. Tabrizi and Dogan Ibrahim, Security of the Internet of Things: An Overview. *Proc. of the 2016 International Conference on Communication and Information Systems*, 146-150, 2016.

[Tekniikka ja talous, 2016] Tekniikka ja talous -lehden verkkoartikkeli: *Ennätyksellisessä kyberhyökkäyksessä käytettiin yli 145 000 kameraa*. Saatavilla sähköisesti: http://www.tekniikkatalous.fi/tekniikka/ennatyksellisessa-kyberhyokkayksessa-kaytettiin-yli-145-000-kameraa-6586663 (viitattu 2.10.2016).

[Tekniikka ja talous, 2017] Tekniikka ja talous -lehden verkkoartikkeli: *Mirai-haittaohjelma riehuu yhä Suomessakin – satoja liittymiä jouduttu sulkemaan*. Saatavilla sähköisesti: http://www.tekniikkatalous.fi/tekniikka/ict/mirai-haittaohjelma-riehuu-yha-suomessakin-satoja-liittymia-jouduttu-sulkemaan-6623299 (viitattu 18.2.2017).

[Tietoviikko, 2016a] Tietoviikko -lehden verkkoartikkeli *Tietoturvafirma varoittaa: tunnettu tv-tikku saattaa vaaraan koko kodin*. Saatavilla sähköisesti: http://www.tivi.fi/Kaikki_uutiset/tietoturvafirma-varoittaa-tunnettu-tv-tikku-saattaa-vaaraan-koko-kodin-6243736 (viitattu 2.10.2016).

[Tietoviikko, 2016b] Tietoviikko-lehden verkkoartikkeli *Kylmentyneineitä kerrostaloja paljastui lisää – hakkerit iskevät lämmitykseen*. Saatavilla sähköisesti: http://www.tivi.fi/Kaikki_uutiset/kylmentyneineita-kerrostaloja-paljastui-lisaa-hakkerit-iskevat-lammitykseen-6598148 (viitattu 26.6.2017).

[Tzezana, 2016] Roey Tzezana, Scenarios for crime and terrorist attacks using the internet of things, 2016. https://link.springer.com/article/10.1007/s40309-016-0107-z (checked 11.7.2017)

[Uusi Suomi, 2011] Uusi Suomi -lehden verkkoartikkeli *Ruma verkkohyökkäys Pekka Haaviston kimppuun - ”Poliisille”*. Saatavilla sähköisesti: https://www.uusisuomi.fi/kotimaa/118981-ruma-verkkohyokkays-pekka-haaviston-kimppuun-%E2%80%9Dpoliisille%E2%80%9D (viitattu 26.6.2017).

[Uusi Suomi, 2012a] Uusi Suomi -lehden verkkoartikkeli *Laaja verkkohyökkäys Suomeen - HS.fi kaatui, Poliisi.fi tökkii*. Saatavilla sähköisesti: https://www.uusisuomi.fi/kotimaa/53406-juuri-nyt-laaja-verkkohyokkays-suomessa (viitattu 26.6.2017).

[Uusi Suomi, 2012b] Uusi Suomi -lehden verkkoartikkeli *Poliisi.fi kaatui ”kuituvikaan”, Sanomaan hyökättiin ulkomailta*. Saatavilla sähköisesti: https://www.uusisuomi.fi/kotimaa/53407-poliisi-ei-verkkohyokkays-vaan-operaattorin-kuituvika (viitattu 26.6.2017).

[Uusi Suomi, 2012c] Uusi Suomi -lehden verkkoartikkeli *Verkkohyökkäys ohi: Uuden Suomen palvelut toimivat taas*. Saatavilla sähköisesti: https://www.uusisuomi.fi/kotimaa/56077-verkkohyokkays-ohi-uuden-suomen-palvelut-toimivat-taas (viitattu 26.6.2017).

[Uusi Suomi, 2015] Uusi Suomi -lehden verkkoartikkeli *Pankkihyökkäyksistä "uusia havaintoja"*. Saatavilla sähköisesti: https://www.uusisuomi.fi/kotimaa/76181-pankkihyokkayksista-uusia-havaintoja (viitattu 26.6.2017).

[Uusi Suomi, 2016] Uusi Suomi -lehden verkkoartikkeli *Kerrostalojen lämmityksiin isketään Suomessa – Tivi: "Potentiaalisia kohteita on satoja"*. Saatavilla sähköisesti: https://www.uusisuomi.fi/asuminen/208116-tivi-kerrostalojen-lammityksiin-isketaan-suomessa-potentiaalisia-kohteita-satoja (viitattu 26.6.2017).

[Valtioneuvosto, 2017] Valtioneuvoston viestintäosaston tiedote: *Eurooppalainen hybridiuhkien osaamiskeskus perustettiin Helsinkiin*. Saatavilla sähköisesti: http://valtioneuvosto.fi/artikkeli/-/asset_publisher/10616/eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin (viitattu 23.6.2017).

[Valtiovarainministeriö, 2003] Valtiovarainministeriö, *Valtion tietohallinnon Internet-tietoturvallisuusohje*. Saatavilla sähköisesti: https://www.vahtiohje.fi/web/guest/1/2003-valtion-tietohallinnon-internet-tietoturvallisuusohje (viitattu 1.6.2017).

[Rydman, 2016] Arno Rydman, Demarimeppi: Euroopan parlamentti suunnittelee scifi-lakeja. *Verkkouutiset.fi*, 2016. Saatavilla sähköisesti: http://www.verkkouutiset.fi/politiikka/miapetra%20kumpula%20natri%20scifi%20lait-56394 (viitattu 14.10.2016).

[Viestintävirasto, 2007] Viestintäviraston Tietoturva nyt! -artikkeli, *Palvelunestohyökkäyksiä on monta lajia*, 2007. Saatavilla sähköisesti: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2007/05/P_12.html (viitattu 7.3.2017).

[Viestintävirasto, 2016a] Viestintäviraston varoitukset. Saatavilla sähköisesti: https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset.html (viitattu 27.10.2016).

[Viestintävirasto, 2016b] Viestintäviraston luettelo ohjelmistojen haavoittuvuuksista. Saatavilla sähköisesti: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet.html (viitattu 27.10.2016).

[Viestintävirasto, 2016c] Viestintäviraston kyberturvallisuuskeskus, Palvelunestohyökkäysten tekniikkaa puolustajille. Saatavilla sähköisesti: https://www.viestintavirasto.fi/attachments/tietoturva/Ohje_3_2016_liite_1_Palvelunestohyokkaysten_tekniikkaa_puolustajille.pdf (viitattu 20.6.2017).

[Viestintävirasto, 2017] Tietoturvan vuosi 2016. Saatavilla sähköisesti: https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf

[Web-opas, 2012] Web-opas, *Mikä on palvelunestohyökkäys*, 2012. Saatavilla sähköisesti: http://www.webopas.net/palvelunestohyokkaus.html (viitattu 7.3.2012).

[Wong, 2016] Joon Ian Wong, Cybercrime is booming and the Internet of Things will just make things worse, 2016. https://qz.com/603996/cybercrime-is-booming-and-the-internet-of-things-will-just-make-things-worse/ (checked 13.7.2017).

[Yle, 2016] Yle.fi-palvelun verkkouutinen *Palvelunestohyökkäykset jumittavat julkishallinnon verkkopalveluita*. Saatavilla sähköisesti: http://yle.fi/uutiset/3-9233094 (viitattu 16.10.2016).

[Zakon, 2003] Robert H Zakon. *Hobbes' internet timeline, version 23, 2016*. http://www.zakon.org/robert/internet/timeline/ (checked 15.9.2016).